Lignes directrices

Lignes directrices 03/2022 relatives aux interfaces trompeuses dans les interfaces des plateformes de médias sociaux: comment les reconnaître et les éviter?

Version 2.0

Adoptées le 14 février 2023

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Historique des versions

Version 2.0	14 février 2023	Adoption des lignes directrices après la consultation publique
Version 1.0	14 mars 2022	Adoption des lignes directrices pour consultation publique

SYNTHÈSE

Les présentes lignes directrices proposent aux fournisseurs de médias sociaux en tant que responsables du traitement des médias sociaux, aux concepteurs et aux utilisateurs de plateformes de médias sociaux, des recommandations pratiques sur la manière de reconnaître et d'éviter ce qu'on appelle les «interfaces trompeuses» dans les interfaces des médias sociaux qui ne respectent pas les exigences du RGPD. À cette fin, le comité européen de la protection des données (ci-après l'«EDPB») recommande aux responsables du traitement de s'appuyer sur des équipes interdisciplinaires composées, notamment, de concepteurs, de délégués à la protection des données et de décideurs. Il importe de faire observer que la liste des interfaces trompeuses et des bonnes pratiques, ainsi que les cas d'utilisation, ne sont pas exhaustifs. Les fournisseurs de médias sociaux demeurent responsables et comptables du respect du RGPD par leurs plateformes.

Interfaces trompeuses dans les interfaces des plateformes de médias sociaux

Dans le cadre des présentes lignes directrices, les «interfaces trompeuses» sont considérées comme des interfaces et des parcours d'utilisateur mis en œuvre sur les plateformes de médias sociaux qui tentent d'inciter les utilisateurs à prendre des décisions involontaires, contre leur gré et potentiellement préjudiciables, souvent contraires à leurs intérêts et favorables aux intérêts des plateformes de médias sociaux, en ce qui concerne le traitement de leurs données à caractère personnel. Les interfaces trompeuses visent à influencer le comportement des utilisateurs et peuvent entraver leur capacité à protéger efficacement leurs données à caractère personnel et à faire des choix en conscience. Les autorités chargées de la protection des données ont pour mission de sanctionner l'utilisation des interfaces trompeuses lorsqu'elles ne respectent pas les exigences du RGPD. Les interfaces trompeuses analysées dans les présentes lignes directrices peuvent être divisées en plusieurs catégories:

- la ***surcharge*** *(overloading):* confronter l'utilisateur à une avalanche ou à une grande quantité de demandes, d'informations, d'options ou de possibilités, afin de l'inciter à partager davantage de données ou à autoriser involontairement un traitement de données à caractère personnel qui va à l'encontre des attentes de la personne concernée.
  Les trois types suivants d'interfaces trompeuses appartiennent à cette catégorie: l'***incitation répétitive*** *(continuous prompting)*, le ***labyrinthe*** *(privacy maze)* et les ***trop nombreuses options*** *(too many options)*

- l'***inattention*** *(skipping):* concevoir l'interface ou le parcours d'utilisateur de telle manière que l'utilisateur omet ou néglige tout ou partie des aspects liés à la protection des données.
  Les deux types suivants d'interfaces trompeuses appartiennent à cette catégorie: le ***confort trompeur*** *(deceptive snugness)* et le ***détournement d'attention*** *(look over there)*

- l'***incitation*** *(stirring):* influencer le choix que ferait l'utilisateur en faisant appel à ses émotions ou en utilisant des indications visuelles («visual nudges»).
  Les deux types suivants d'interfaces trompeuses appartiennent à cette catégorie: le ***pilotage émotionnel*** *(emotional steering)* et la technique du ***caché au grand jour*** *(hidden in plain sight)*

- l'***obstruction:*** (*obstructing*) entraver ou bloquer l'utilisateur dans son processus de recherche d'informations ou de gestion de ses données en rendant l'action difficile ou impossible à exécuter.
  Les trois types suivants d'interfaces trompeuses appartiennent à cette catégorie: l'***impasse*** (*dead end*), le ***processus plus long que nécessaire*** (*longer than necessary*) et l'***action trompeuse*** (*misleading action*)

- l'***inconstance:*** (*fickle*) concevoir des interfaces qui prêtent à confusion ou sont peu claires, ce qui rend difficile pour l'utilisateur de naviguer dans les différents outils de contrôle de la protection des données et de comprendre la finalité du traitement.
  Les quatre types suivants d'interfaces trompeuses appartiennent à cette catégorie: le ***manque de hiérarchie*** *(lacking hierarchy)****, la décontextualisation*** *(decontextualising),* ***l'interface incohérente*** *(inconsistent interface)* et la ***discontinuité linguistique*** (*language discontinuity*)

- le ***brouillage:*** (*left in the dark*) une interface est conçue de manière à dissimuler des informations ou des outils de contrôle de la protection des données, ou à laisser l'utilisateur dans l'incertitude quant à la façon dont ses données sont traitées et au type de contrôle qu'il pourrait avoir sur ce traitement dans le cadre de l'exercice de ses droits.
  Les deux types suivants d'interfaces trompeuses appartiennent à cette catégorie: les ***nformations contradictoires*** (*conflicting information*) et les ***formulations ou informations ambiguës*** (*ambiguous wording or information*)

Dispositions du RGPD pertinentes aux fins de l'appréciation des interfaces trompeuses

En ce qui concerne le respect de la protection des données par les interfaces utilisateur des applications en ligne dans le secteur des médias sociaux, les principes applicables en matière de protection des données sont énoncés à l'article 5 du RGPD. Le principe de traitement loyal énoncé à l'article 5, paragraphe 1, point a), du RGPD sert de point de départ pour déterminer si une interface constitue effectivement une «interface trompeuse». Les autres principes intervenant dans cette appréciation sont la transparence, la minimisation des données et la responsabilité au titre de l'article 5, paragraphe 1, points a) et c), et de l'article 5, paragraphe 2, du RGPD, ainsi que, dans certains cas, la limitation des finalités au titre de l'article 5, paragraphe 1, point b), du RGPD. Dans d'autres cas, l'appréciation juridique est également fondée sur des conditions relatives au consentement énoncées à l'article 4, paragraphe 11, et à l'article 7 du RGPD, ou sur d'autres obligations spécifiques, telles que l'article 12 du RGPD. De toute évidence, dans le cadre des droits conférés à la personne concernée, il convient de prendre également en considération le troisième chapitre du RGPD. Enfin, les exigences en matière de protection des données dès la conception et de protection des données par défaut prévues à l'article 25 du RGPD jouent un rôle essentiel, car leur application avant le lancement d'une interface pourrait aider les fournisseurs de médias sociaux à éviter les interfaces trompeuses.

Exemples d'interfaces trompeuses dans des cas d'utilisation du cycle de vie d'un compte sur les médias sociaux

Les dispositions du RGPD s'appliquent à l'ensemble du processus de traitement des données à caractère personnel dans le cadre de l'exploitation des plateformes de médias sociaux, c'est-à-dire à l'intégralité du cycle de vie d'un compte d'utilisateur. L'EDPB donne des exemples concrets de types

d'interfaces trompeuses pour les différents cas d'utilisation suivants au cours de ce cycle de vie: l'inscription, c'est-à-dire la procédure d'enregistrement; les cas d'utilisation des informations concernant la déclaration de confidentialité, la responsabilité conjointe du traitement et la communication de violations de données; le consentement et la gestion de la protection des données; l'exercice des droits des personnes concernées lors de l'utilisation des médias sociaux; et, enfin, la clôture d'un compte sur les médias sociaux. Les liens avec les dispositions du RGPD sont expliqués de deux manières: premièrement, chaque cas d'utilisation explique de façon plus détaillée quelles sont les dispositions du RGPD susmentionnées qui sont particulièrement pertinentes pour lui. Deuxièmement, les points concernant les exemples d'interfaces trompeuses expliquent en quoi ces derniers constituent une violation du RGPD.

Recommandations des bonnes pratiques

Outre les exemples d'interfaces trompeuses, les présentes lignes directrices proposent également des bonnes pratiques à la fin de chaque cas d'utilisation, ainsi qu'à l'annexe II. Celles-ci contiennent des recommandations spécifiques en vue de la conception d'interfaces utilisateur qui facilitent l'application effective du RGPD.

Liste de contrôle des catégories d'interfaces trompeuses

Une liste de contrôle des catégories d'interfaces trompeuses est proposée à l'annexe I des présentes lignes directrices. Elle donne un aperçu général des catégories et des types d'interfaces trompeuses susmentionnés, ainsi qu'une liste des exemples pour chaque interface trompeuse mentionnée dans les cas d'utilisation. Certains lecteurs jugeront peut-être utile d'utiliser la liste de contrôle comme point de départ pour découvrir les présentes lignes directrices.

Table des matières

1 Champ d'application 9

2 Principes applicables – Que faut-il garder à l'esprit? 13

2.1 Responsabilité 14

2.2 Transparence 14

2.3 Protection des données dès la conception et protection des données par défaut 15

3 Le cycle de vie d'un compte sur les médias sociaux: mise en pratique des principes 17

3.1 Ouverture d'un compte sur les médias sociaux 17

Cas d'utilisation n° 1: enregistrement d'un compte 17

3.2 S'informer sur les réseaux sociaux 30

Cas d'utilisation n° 2a: une déclaration de confidentialité à plusieurs niveaux 30

Cas d'utilisation n° 2b: fournir à la personne concernée des informations sur la responsabilité conjointe du traitement (article 26, paragraphe 2, du RGPD) 37

Cas d'utilisation 2c: communication à la personne concernée d'une violation de données à caractère personnel 39

3.3 Se protéger sur les réseaux sociaux 42

Cas d'utilisation n° 3a: gérer son consentement lors de l'utilisation d'une plateforme de médias sociaux 42

Cas d'utilisation n° 3b: gestion de ses paramètres de protection des données 50

3.4 Bien se comporter sur les réseaux sociaux: les droits des personnes concernées 58

Cas d'utilisation n° 4: comment fournir des fonctions appropriées pour l'exercice des droits des personnes concernées 58

3.5 Au revoir et adieu: quitter un compte sur les médias sociaux 66

Cas d'utilisation n° 5: suspension du compte/effacement de toutes les données à caractère personnel 66

4 Annexe I: liste des catégories et types d'interfaces trompeuses 76

4.1 Surcharge 76

4.1.1 Incitation répétitive 76

4.1.2 Labyrinthe 76

4.1.3 Trop nombreuses options 77

4.2 Inattention 77

4.2.1 Confort trompeur 77

4.2.2 Détournement d'attention 78

4.3 Incitation 78

4.3.1 Pilotage émotionnel 78

4.3.2 Caché au grand jour 79

4.4 Obstruction 79
4.4.1 Impasse 79
4.4.2 Processus plus long que nécessaire 80
4.4.3 Action trompeuse 80
4.5 Inconstance 80
4.5.1 Manque de hiérarchie 80
4.5.2 Décontextualisation 81
4.5.3 Interface incohérente 81
4.5.4 Discontinuité linguistique 81
4.6 Brouillage 82
4.6.1 Informations contradictoires 82
4.6.2 Formulations ou informations ambiguës 82
5 Annexe II: Bonnes pratiques 84

Le comité européen de la protection des données,

vu l'article 70, paragraphe 1, point e), du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après le «RGPD»),

vu l'accord sur l'Espace économique européen (EEE), et notamment son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018[1],

vu les articles 12 et 22 de son règlement intérieur,

A ADOPTE LES LIGNES DIRECTRICES SUIVANTES

1 CHAMP D'APPLICATION

1. L'objectif des présentes lignes directrices est de fournir des recommandations et des orientations pour la conception des interfaces des plateformes de médias sociaux. Aux fins des présentes lignes directrices, on entend par médias sociaux les plateformes en ligne qui permettent le développement de réseaux et de communautés d'utilisateurs, via lesquels des informations et des contenus sont partagés[2]. Les lignes directrices peuvent être utilisées soit lors de la phase de conception d'une interface utilisateur, afin d'éviter dès le départ la mise en œuvre d'interfaces trompeuses[3], soit sur un service existant, afin d'évaluer la conformité de son interface. Elles s'adressent aux fournisseurs de médias sociaux en tant que responsables du traitement sur les médias sociaux, qui sont chargés de la conception et de l'exploitation des plateformes de médias sociaux. À cet égard, les lignes directrices visent à rappeler les obligations découlant du RGPD, en ce qui concerne plus particulièrement les principes de licéité, de loyauté, de transparence, de limitation des finalités et de minimisation des données lors de la conception des interfaces utilisateur et de la présentation du contenu de leurs services et applications internet. Les principes susmentionnés doivent être mis en œuvre de façon substantielle et, d'un point de vue technique, ils constituent des exigences pour la conception des logiciels et des services, y compris des interfaces utilisateur. Les lignes directrices présentent une analyse approfondie des exigences du RGPD lorsqu'elles sont appliquées aux interfaces utilisateur et à la présentation de contenu, et expliqueront ce qu'il convient de considérer comme une «interface trompeuse», une façon de concevoir et de présenter du contenu qui viole substantiellement ces exigences, tout en prétendant s'y conformer formellement. Elles sont également un bon moyen de sensibiliser davantage les utilisateurs à leurs droits, ainsi qu'aux risques que peut engendrer le partage d'un trop grand nombre de données ou le partage incontrôlé de leurs données. Les présentes lignes directrices ont également pour but d'apprendre aux utilisateurs à reconnaître les «interfaces

[1] Dans le présent document, on entend par «États membres» les «États membres de l'EEE».

[2] Définition identique à celle donnée dans les lignes directrices 08/2020 de l'EDPB sur le ciblage des utilisateurs de médias sociaux, point 1 (voir la note de bas de page 1 pour une description plus détaillée), consultables à l'adresse suivante: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf

[3] Dans la version 2.0 des présentes lignes directrices, l'EDPB utilise le terme «interface trompeuse», plus inclusif et descriptif, au lieu d'«interface truquée».

trompeuses» (telles que définies ci-après) et à savoir comment y faire face de façon à protéger leur vie privée en conscience. Dans le cadre de cette analyse, le cycle de vie d'un compte sur les médias sociaux a été étudié sur la base de cinq cas d'utilisation: «Ouvrir un compte sur les médias sociaux» (cas d'utilisation n° 1), «S'informer sur les médias sociaux» (cas d'utilisation n° 2), «Se protéger sur les médias sociaux» (cas d'utilisation n° 3), «Bien se comporter sur les médias sociaux: droits des personnes concernées» (cas d'utilisation n° 4) et «Au revoir et adieu: quitter un compte sur les médias sociaux» (cas d'utilisation n° 5).

2. Dans les présentes lignes directrices, le terme «interface utilisateur» correspond au moyen permettant aux personnes d'interagir avec les plateformes de médias sociaux. Le présent document se concentre sur les interfaces utilisateur graphiques (par exemple, celles utilisées pour les interfaces des ordinateurs et des smartphones), mais certaines des observations peuvent également s'appliquer aux interfaces vocales (par exemple, celles utilisées pour les enceintes intelligentes) ou aux interfaces gestuelles (par exemple, celles utilisées dans la réalité virtuelle). Le terme «parcours d'utilisateur» correspond à la série d'actions ou d'étapes que l'utilisateur doit effectuer pour atteindre son objectif, qui, sur les réseaux sociaux, peut consister à parcourir son fil d'actualité, partager un message, définir ses préférences, etc. Le terme «expérience utilisateur» correspond à l'expérience globale de l'utilisateur sur les plateformes de médias sociaux, qui comprend l'utilité perçue, la facilité d'utilisation et l'efficacité de l'interaction avec la plateforme. La conception de l'interface utilisateur et la conception de l'expérience utilisateur n'ont cessé d'évoluer au cours des dix dernières années. Depuis peu, elles offrent à l'utilisateur des interactions et des expériences ubiquitaires, personnalisées et sans ruptures: l'interface parfaite doit être hautement personnalisée, facile à utiliser et multimodale[4]. Bien que ces tendances puissent faciliter l'utilisation des services numériques, elles peuvent être utilisées d'une manière qui encourage surtout l'utilisateur à adopter des comportements allant à l'encontre de l'esprit du RGPD[5]. Cela est particulièrement important dans le contexte de l'économie de l'attention, dans laquelle l'attention de l'utilisateur est considérée comme une marchandise. Dans ces cas, les limites légalement autorisées du RGPD peuvent être outrepassées, et les interfaces et expériences utilisateur dont la conception conduit à de telles situations sont décrites ci-dessous comme des «interfaces trompeuses».

3. Dans le cadre des présentes lignes directrices, les «interfaces trompeuses» sont considérées comme des interfaces et des parcours d'utilisateur mis en œuvre sur les plateformes de médias sociaux qui visent à inciter les utilisateurs à prendre des décisions involontaires, contre leur gré et potentiellement préjudiciables, souvent contraires à leurs intérêts et favorables aux intérêts des plateformes de médias sociaux, en ce qui concerne le traitement de leurs données à caractère personnel. Les interfaces trompeuses visent à influencer le comportement des utilisateurs, généralement en s'appuyant sur des biais cognitifs, et peuvent entraver leur capacité à «protéger efficacement leurs données personnelles et à effectuer des choix en conscience»[6], par exemple en faisant en sorte qu'ils n'aient pas les moyens de «donner un consentement libre et éclairé»[7]. Ces biais peuvent être exploités dans plusieurs aspects de la conception, tels que le choix des couleurs des interfaces et l'emplacement du contenu. À

[4] Pour en savoir plus, voir CNIL, cahiers IP, nº 6: *La forme des choix*, 2019. p. 9, à l'adresse suivante: https://cnil.fr/sites/cnil/files/atoms/files/cnil_cahiers_ip6.pdf

[5] CNIL, *La forme des choix*, 2019. p. 10.

[6] CNIL, *La forme des choix*, 2019. p. 27.

[7] Voir Norwegian Consumer Council (Conseil norvégien des consommateurs), *Deceived by design*: *How tech companies use dark patterns to discourage us from exercising our rights to privacy*, (comment les entreprises technologiques utilisent les interfaces trompeuses pour nous dissuader d'exercer nos droits à la vie privée), p. 10: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf; mais aussi CNIL, *La forme des choix*, p. 30 et 31.

l'inverse, les incitations et les conceptions conviviales peuvent favoriser la mise en œuvre de la réglementation en matière de protection des données.

4. Les interfaces trompeuses ne conduisent pas nécessairement à une violation de la seule réglementation en matière de protection des données. Elles peuvent, par exemple, enfreindre également la réglementation en matière de protection des consommateurs. Les limites entre les violations sanctionnées par les autorités chargées de la protection des données et celles sanctionnées par les autorités nationales chargées de la protection des consommateurs, de la concurrence ou d'autres autorités peuvent se chevaucher[8]. Selon le RGPD, il incombe aux autorités chargées de la protection des données de sanctionner l'utilisation d'interfaces trompeuses si celles-ci violent effectivement les normes en matière de protection des données et, partant, le RGPD. Les violations des exigences du RGPD doivent être appréciées au cas par cas. Seules les interfaces trompeuses susceptibles de relever de ce mandat réglementaire sont couvertes par les présentes lignes directrices. C'est pourquoi, outre des exemples d'interfaces trompeuses, les lignes directrices présentent également les bonnes pratiques pouvant être appliquées pour concevoir des interfaces utilisateur qui facilitent la mise en œuvre effective du RGPD. Ces bonnes pratiques peuvent constituer une première étape vers la création d'une solution uniformisée permettant à l'utilisateur de contrôler efficacement ses données et d'exercer ses droits.

5. Les interfaces trompeuses[9] décrites dans les présentes lignes directrices résultent d'une analyse interdisciplinaire des interfaces existantes et peuvent être réparties dans les catégories suivantes:

Surcharge *(overloading):* l'utilisateur est confronté à une avalanche ou à une grande quantité de demandes, d'informations, d'options ou de possibilités, afin de l'inciter à partager davantage de données ou à autoriser involontairement un traitement des données à caractère personnel qui va à l'encontre des attentes de la personne concernée.

Inattention *(skipping):* concevoir l'interface ou le parcours d'utilisateur de telle manière que les utilisateurs omettent ou négligent tout ou partie des aspects liés à la protection des données.

Incitation *(stirring):* influence le choix que ferait l'utilisateur en faisant appel à ses émotions ou en utilisant des indications visuelles («visual nudges»).

Obstruction *(obstructing):* entraver ou bloquer les utilisateurs dans leur processus d'information ou de gestion de leurs données en rendant l'action difficile ou impossible à réaliser.

Inconstance *(fickle):* la conception de l'interface prête à confusion ou est peu claire, ce qui rend difficile pour l'utilisateur de naviguer dans les différents outils de contrôle de la protection des données et de comprendre la finalité du traitement.

[8] À cet égard, l'article 25, paragraphe 2, du règlement (UE) 2022/2065 du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) précise que l'interdiction de concevoir les interfaces en ligne de façon à tromper ou à manipuler énoncée à l'article 25, paragraphe 1, ne s'applique pas aux pratiques couvertes par la directive 2005/29/CE (directive relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs, ci-après la «directive sur les pratiques commerciales déloyales») ou le RGPD. En outre, la communication de la Commission (2021/C 526/01) propose, à sa section 4.2.7, des orientations concernant l'interprétation et l'application de la directive sur les pratiques commerciales déloyales, y compris sur les «interfaces truquées».

[9] Les catégories d'interfaces trompeuses et les types d'interfaces trompeuses au sein de ces catégories seront indiqués en ***caractères gras et italiques*** dans le texte des lignes directrices. Une vue d'ensemble détaillée est présentée en annexe.

Brouillage *(left in the dark):* une interface est conçue de manière à dissimuler des informations ou des outils de contrôle de la protection des données, ou à laisser l'utilisateur dans l'incertitude quant à la manière dont ses données sont traitées et au type de contrôle qu'il pourrait avoir sur ce traitement dans le cadre de l'exercice de ses droits.

6. Outre le regroupement des interfaces trompeuses sous ces catégories en fonction de leurs effets sur le comportement de l'utilisateur, ces interfaces peuvent également être divisées en interfaces trompeuses fondées sur le contenu et en interfaces trompeuses fondées sur le processus de navigation afin de traiter plus spécifiquement certains aspects de l'interface utilisateur ou du parcours utilisateur. Les interfaces trompeuses fondées sur le contenu se rapportent au contenu proprement dit, et donc également à la formulation et au contexte des phrases et des éléments d'information. Toutefois, il existe également des éléments qui ont une influence directe sur la perception de ces facteurs. Ces interfaces trompeuses fondées sur le processus de navigation sont liées à la façon d'afficher le contenu, de naviguer dans celui-ci ou d'interagir avec lui.

7. Il est essentiel de garder à l'esprit que les interfaces trompeuses suscitent également des inquiétudes quant à leur incidence potentielle sur les enfants[10] qui s'inscrivent sur la plateforme de médias sociaux, ainsi que sur d'autres groupes de personnes vulnérables telles que les personnes âgées, les personnes malvoyantes ou les personnes qui n'ont pas les mêmes compétences numériques que d'autres. Les groupes vulnérables, tels que les personnes âgées, sont souvent non seulement moins aptes à reconnaître les pratiques de conception manipulatrice, mais aussi moins conscients du fait que leur comportement numérique subit une influence. Le RGPD exige des garanties supplémentaires lorsque le traitement concerne les données à caractère personnel d'enfants, ceux-ci pouvant être moins conscients des risques et des conséquences concernés et de leurs droits liés au traitement[11]. Le considérant 58 indique expressément que lorsque le traitement concerne un enfant, toute information devrait être rédigée en termes clairs et simples que l'enfant peut aisément comprendre. En outre, le RGPD inclut explicitement le traitement des données des personnes physiques, en particulier celles des enfants, dans les situations dans lesquelles des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données à caractère personnel qui est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral[12].

8. Eu égard à ce qui précède, il faut bien comprendre que les interfaces trompeuses ne sont pas propres aux plateformes de médias sociaux. Des avis très fermes ont été exprimés à ce sujet lors de la consultation publique sur les présentes lignes directrices. Les interfaces sont présentes dans de nombreuses autres situations dans lesquelles l'utilisateur interagit avec des produits et des services fondés sur des opérations de traitement de données, ou liés à celles-ci. Il peut s'agir, par exemple, de sites internet et de bandeaux relatifs aux cookies[13], de boutiques en ligne, de jeux vidéo, d'applications

---

[10] Voir également le considérant 81, quatrième phrase, du règlement (UE) 2022/2065 (règlement sur les services numériques).

[11] Considérant 38 du RGPD.

[12] Considérant 75 du RGPD; voir également les lignes directrices 08/2020 de l'EDPB sur le ciblage des utilisateurs de médias sociaux, point 16, consultables à l'adresse suivante: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf

[13] En raison d'une série de réclamations introduites par une organisation autrichienne de protection de la vie privée (NOYB), un groupe de travail de l'EDPB a procédé à un échange de vues sur plusieurs éléments de conception des bandeaux relatifs aux cookies. Le dénominateur commun sur lequel se sont accordées les autorités de contrôle dans leur interprétation du cadre juridique applicable à plusieurs niveaux a été résumé

et de micropaiements mobiles, etc. Bien que les interfaces trompeuses décrites ci-dessous n'apparaissent pas toujours sous une forme rigoureusement identique, leurs variantes peuvent aussi porter atteinte aux droits des personnes concernées ou des consommateurs. Néanmoins, les présentes lignes directrices se concentrent uniquement sur les interfaces trompeuses sur les plateformes de médias sociaux, car l'influence de ces plateformes sur la vie quotidienne des personnes et des pays ne cesse de croître, ce qui a été clairement établi dans de précédents documents de l'EDPB[14].

2 PRINCIPES APPLICABLES – QUE FAUT-IL GARDER A L'ESPRIT?

9. En ce qui concerne le respect de la protection des données par les interfaces utilisateur des applications en ligne dans le secteur des médias sociaux, les principes applicables en matière de protection des données sont énoncés à l'article 5 du RGPD. Le principe de traitement loyal énoncé à l'article 5, paragraphe 1, point a), du RGPD est le point de départ pour déterminer s'il existe des interfaces trompeuses. Comme l'EDPB l'a déjà indiqué, la loyauté est un principe fondamental selon lequel les données à caractère personnel ne doivent pas être traitées d'une manière préjudiciable ou discriminatoire, inattendue ou trompeuse pour la personne concernée[15]. Si l'interface contient des informations insuffisantes ou trompeuses pour l'utilisateur et présente les caractéristiques d'une interface trompeuse, elle peut être considérée comme un traitement déloyal. Le principe de loyauté a une fonction générique et toutes les interfaces trompeuses ne le respecteraient pas, indépendamment du respect d'autres principes relatifs à la protection des données.

10. Outre cette disposition fondamentale concernant la loyauté du traitement, les principes de responsabilité et de transparence ainsi que l'obligation de protection des données dès la conception énoncés à l'article 25 du RGPD sont également pertinents en ce qui concerne le cadre de conception, et les interfaces trompeuses pourraient violer ces dispositions. Toutefois, l'appréciation juridique des interfaces trompeuses peut également être fondée sur les éléments des définitions générales telles que la définition du consentement présentée à l'article 4, point 11, du RGPD, ou d'autres obligations spécifiques telles que celles prévues à l'article 12 du RGPD. L'article 12, paragraphe 1, première phrase, du RGPD exige des responsables du traitement qu'ils prennent des mesures appropriées pour procéder à toute communication relative aux droits des personnes concernées, ainsi que pour fournir toute information, d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples. Comme l'indique la troisième phrase du considérant 39 sur le principe de transparence, cette exigence n'est toutefois pas limitée aux avis de protection de la vie privée[16] ou aux

dans un rapport intitulé «Report of the work undertaken by the Cookie Banner Taskforce» (rapport des travaux entrepris par le groupe de travail sur les bandeaux relatifs aux cookies), publié le 17 janvier 2023 et disponible à l'adresse suivante: https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf

[14] Lignes directrices 08/2020 de l'EDPB sur le ciblage des utilisateurs de médias sociaux, déclaration 2/2019 sur l'utilisation des données à caractère personnel dans le cadre de campagnes politiques, consultables à l'adresse suivante: https://www.edpb.europa.eu/sites/default/files/files/file1/201902_edpb_statementonelections_fr.pdf

[15] Voir les lignes directrices 04/2019 relatives à l'article 25 – Protection des données dès la conception et protection des données par défaut, version 2.0, adoptées le 20 octobre 2020, p. 16. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_fr

[16] Traités dans la partie 3.2. – cas d'utilisation 2a des présentes lignes directrices.

droits des personnes concernées[17], mais s'applique à toute information et communication relatives au traitement de données à caractère personnel. La cinquième phrase de ce considérant précise également que les personnes concernées devraient être informées des risques, règles, garanties et droits liés au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en ce qui concerne ce traitement.

11. En ce qui concerne la conception des interfaces utilisateur des applications en ligne, il importe également de tenir compte du principe de limitation des finalités prévu à l'article 5, paragraphe 1, point b), du RGPD, ainsi que du principe de minimisation des données énoncé à l'article 5, paragraphe 1, point c), du RGPD. En tout état de cause, afin de garantir le respect de la protection des données, il est vivement conseillé aux responsables du traitement de procéder à une double vérification de la conformité avec tous les principes relatifs à la protection des données énoncés dans le RGPD.

2.1 Responsabilité

12. Le principe de responsabilité doit être pris en compte dans la conception de chaque interface utilisateur.

13. L'article 5, paragraphe 2, du RGPD dispose que le responsable du traitement est responsable du respect des principes décrits à l'article 5, paragraphe 1, du RGPD et est en mesure de démontrer que ceux-ci sont respectés. Ce principe est donc étroitement lié aux principes pertinents susmentionnés. La responsabilité peut être démontrée par des éléments prouvant que le fournisseur de médias sociaux respecte le RGPD. L'interface utilisateur et le parcours d'utilisateur peuvent servir d'outil de documentation pour démontrer que l'utilisateur, lors de ses actions sur la plateforme de médias sociaux, a lu et pris en considération les informations relatives à la protection des données, a donné librement son consentement, a pu aisément exercer ses droits, etc. Les méthodes qualitatives et quantitatives de recherche sur les utilisateurs, telles que les tests A/B, l'oculométrie ou les entretiens avec les utilisateurs, ainsi que leurs résultats et leur analyse peuvent être utilisés pour démontrer la conformité. Il importe de faire observer que ces méthodes de recherche supposent souvent elles-mêmes le traitement de données à caractère personnel, qui doit donc être conforme au RGPD. Si, par exemple, l'utilisateur doit cocher une case ou cliquer sur une option de protection des données parmi plusieurs, les captures d'écran des interfaces peuvent servir à montrer le parcours de l'utilisateur à travers les informations relatives à la protection des données et à expliquer comment celui-ci prend une décision éclairée. Les résultats de la recherche sur les utilisateurs effectuée sur cette interface apporteraient des éléments supplémentaires expliquant en quoi l'interface est optimale pour atteindre un objectif d'information.

14. Dans le domaine des interfaces utilisateur, ces éléments documentaires peuvent figurer dans la divulgation de certains accords et, surtout, lors de l'obtention de preuves, par exemple d'un consentement donné ou d'une confirmation de lecture.

2.2 Transparence

15. Le principe de transparence énoncé à l'article 5, paragraphe 1, point a), du RGPD recouvre en grande partie le domaine de la responsabilité générale. Bien que les responsables du traitement doivent protéger certaines informations commerciales sensibles à l'égard de tiers, le fait de rendre la documentation relative au traitement accessible ou enregistrable pourrait contribuer à la responsabilité: par exemple, une confirmation de lecture peut être obtenue pour un texte que le

[17] Traités dans les cas d'utilisation 4 et 5, c'est-à-dire les parties 3.4 et 3.5 des présentes lignes directrices.

responsable du traitement est tenu de divulguer en vertu du principe de transparence. Cela peut toujours servir, en même temps, à garantir la transparence à l'égard des personnes concernées.

16. Tous les principes relatifs à la protection des données énoncés à l'article 5 du RGPD sont décrits de façon plus précise dans le RGPD. L'article 5, paragraphe 1, point a), du RGPD prévoit que les données à caractère personnel sont traitées de manière transparente au regard de la personne concernée. Les lignes directrices sur la transparence précisent les éléments de transparence énoncés à l'article 12 du RGPD, à savoir la nécessité de fournir les informations «d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples»[18]. Les présentes lignes directrices fournissent également des orientations sur la manière de se conformer aux obligations d'information prévues aux articles 13 et 14 du RGPD en ce qui concerne les fournisseurs de médias sociaux.

17. En outre, le texte des principes relatifs à la protection des données énoncés à l'article 5, paragraphe 1, point a), du RGPD et d'autres dispositions juridiques particulières du règlement contiennent beaucoup plus de détails sur le principe de transparence, qui sont liés à des principes juridiques spécifiques, tels que les exigences particulières de transparence énoncées à l'article 7 du RGPD relatif à l'obtention du consentement.

2.3 Protection des données dès la conception et protection des données par défaut

18. L'article 25, paragraphe 1, du RGPD dispose que le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, tandis que l'article 25, paragraphe 2, précise que ces mesures doivent également être mises en œuvre pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique de traitement sont traitées. Dans le cadre des lignes directrices 04/2019 relatives à l'article 25 – Protection des données dès la conception et protection des données par défaut, les responsables du traitement et les sous-traitants doivent tenir compte de certains éléments clés lors de la mise en œuvre de la protection des données dès la conception concernant une plateforme de médias sociaux. L'un de ces éléments est, en ce qui concerne le principe de loyauté, que les informations et les options relatives au traitement des données devraient être fournies d'une manière objective et neutre, en évitant tout langage ou toute conception trompeurs ou manipulateurs[19]. Les lignes directrices mettent en évidence les éléments des principes relatifs à la protection des données par défaut et à la protection des données dès la conception, entre autres, qui deviennent encore plus pertinents lorsqu'il s'agit d'interfaces trompeuses[20]:

- Autonomie – Les personnes concernées devraient se voir accorder le degré d'autonomie le plus élevé possible pour déterminer l'utilisation qui est faite des données à caractère personnel les concernant, ainsi que la portée et les conditions de cette utilisation ou de ce traitement.

[18] Lignes directrices du groupe de travail «Article 29» sur la transparence au sens du règlement (UE) 2016/679, approuvées par l'EDPB: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
[19] Lignes directrices 04/2019 relatives à l'article 25 – Protection des données dès la conception et protection des données par défaut, p. 18, point 70.
[20] Extrait – pour la liste complète, voir les lignes directrices 04/2019 relatives à l'article 25 – Protection des données dès la conception et protection des données par défaut, point 70.

- Interaction – Les personnes concernées doivent être en mesure de communiquer et d'exercer leurs droits auprès du responsable du traitement en ce qui concerne les données à caractère personnel traitées par ce dernier.
- Attentes – Le traitement devrait correspondre aux attentes raisonnables des personnes concernées.
- Choix du consommateur – Le responsable du traitement ne devrait pas «engager» ses utilisateurs d'une manière déloyale. Lorsqu'un service traitant des données à caractère personnel est exclusif, il peut créer un engagement à l'égard du service qui peut ne pas être loyal s'il entrave la possibilité pour les personnes concernées d'exercer leur droit de portabilité des données visé à l'article 20 du RGPD.
- Équilibre de pouvoir – L'équilibre de pouvoir devrait être un objectif central de la relation entre le responsable du traitement et la personne concernée. Les déséquilibres de pouvoir devraient être évités. Lorsque cela n'est pas possible, ces déséquilibres devraient être reconnus et pris en compte dans le cadre de contre-mesures appropriées.
- Absence de tromperie – Les informations et les options relatives au traitement des données devraient être fournies d'une manière objective et neutre, en évitant tout langage ou toute conception trompeurs ou manipulateurs.
- Véracité – Le responsable du traitement doit mettre à disposition des informations sur la manière dont il traite les données à caractère personnel, et il doit agir conformément à ses engagements et ne pas induire les personnes concernées en erreur.

19. Le respect des principes relatifs à la protection des données par défaut et à la protection des données dès la conception a toute son importance lors de l'appréciation des interfaces trompeuses, étant donné qu'il permettrait tout simplement de les éviter. En effet, l'analyse de son service et des interfaces qui y sont liées au regard des éléments constitutifs des principes relatifs à la protection des données par défaut et à la protection des données dès la conception, tels que ceux mentionnés ci-dessus, permettra de déterminer, préalablement au lancement du service, si certains aspects de celui-ci constituent une interface trompeuse. Par exemple, si les informations relatives à la protection des données ne sont pas fournies conformément au principe «Absence de tromperie», il est probable qu'elles constituent une interface trompeuse de type ***caché au grand jour*** ou ***pilotage émotionnel***, qui seront développés plus avant dans le cas d'utilisation 1.

3 LE CYCLE DE VIE D'UN COMPTE SUR LES MEDIAS SOCIAUX: MISE EN PRATIQUE DES PRINCIPES

20. Le RGPD s'applique à l'ensemble du processus de traitement automatisé des données à caractère personnel[21]. Cela signifie, dans le cas d'un traitement de données à caractère personnel effectué dans le cadre de l'exploitation de plateformes de médias sociaux, que le RGPD et ses principes s'appliquent à l'intégralité du cycle de vie d'un compte d'utilisateur.

3.1 Ouverture d'un compte sur les médias sociaux

Cas d'utilisation n° 1: enregistrement d'un compte

a. Description du contexte

21. La première démarche que l'utilisateur doit effectuer pour avoir accès à une plateforme de médias sociaux consiste à s'inscrire en créant un compte. Au cours de la procédure d'enregistrement, il est invité à communiquer ses données à caractère personnel, telles que ses nom et prénom, son adresse électronique ou, parfois, son numéro de téléphone. L'utilisateur doit être informé du traitement de ses données à caractère personnel et est généralement invité à confirmer qu'il a lu la déclaration de confidentialité et qu'il accepte les conditions d'utilisation de la plateforme. Ces informations doivent lui être fournies dans des termes simples et clairs, afin qu'il soit en mesure de les comprendre aisément et de les accepter en toute connaissance de cause.

22. Au cours de cette première étape du processus d'inscription, l'utilisateur devrait pouvoir comprendre ce à quoi il s'engage exactement, c'est-à-dire que l'objet de l'accord entre la plateforme de médias sociaux et l'utilisateur devrait être décrit de la manière la plus claire et la plus simple possible.

23. Par conséquent, les fournisseurs de médias sociaux doivent tenir compte de façon effective de la protection des données dès la conception afin de protéger les droits et libertés des personnes concernées[22].

b. Dispositions juridiques pertinentes

24. Les fournisseurs de médias sociaux doivent veiller à mettre en œuvre les principes énoncés à l'article 5 du RGPD de façon appropriée lors de la conception de leurs interfaces. Si la transparence à l'égard des personnes concernées est toujours essentielle, elle l'est particulièrement au moment de la création d'un compte sur une plateforme de médias sociaux. En leur qualité de responsable du traitement ou de sous-traitant, les plateformes de médias sociaux devraient présenter les informations à l'utilisateur de façon efficace et succincte lors de son inscription, et les différencier clairement des autres informations qui ne sont pas liées à la protection des données[23]. Une partie des obligations de transparence incombant aux responsables du traitement concerne l'information de l'utilisateur quant à ses droits, dont le droit de retirer son consentement à tout moment si celui-ci constitue la base juridique applicable[24].

[21] Voir article 2, paragraphe 1, du RGPD.
[22] Voir les lignes directrices 04/2019 relatives à l'article 25 – Protection des données dès la conception et protection des données par défaut.
[23] Voir point 8 des lignes directrices sur la transparence.
[24] Point 30 et page 39 des lignes directrices sur la transparence.

i. Consentement donné au stade du processus d'inscription

25. Comme l'indiquent l'article 4, paragraphe 11, et l'article 7 du RGPD, précisés par le considérant 32, lorsque le consentement est choisi comme fondement juridique du traitement, il doit s'agir d'une «*manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement*». Toutes ces exigences doivent être satisfaites de manière cumulative pour que le consentement soit considéré comme valable.

26. Pour les fournisseurs de médias sociaux qui demandent le consentement de l'utilisateur à différentes fins de traitement, les lignes directrices 05/2020 de l'EDPB sur le consentement fournissent des orientations précieuses sur l'obtention du consentement[25]. Les plateformes de médias sociaux ne doivent pas contourner les conditions, telles que la capacité des personnes concernées à donner librement leur consentement, par des conceptions graphiques ou des formulations qui empêcheraient les personnes concernées d'exercer cette volonté. À cet égard, l'article 7, paragraphe 2, du RGPD prévoit que la demande de consentement est présentée sous une forme qui la distingue clairement des autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Les utilisateurs de plateformes de médias sociaux peuvent donner leur consentement pour des annonces ou des types particuliers d'analyse au cours du processus d'inscription, ainsi qu'à un stade ultérieur, via les paramètres de protection des données. En tout état de cause, comme le souligne le considérant 32 du RGPD, le consentement doit toujours être donné par un acte positif clair, de sorte que les cases cochées par défaut ou l'inactivité de l'utilisateur ne constituent pas un consentement[26].

27. Comme l'EDPB l'a déjà souligné dans ses lignes directrices sur le consentement, pour que le seuil de consentement «éclairé» soit atteint, l'utilisateur doit recevoir un minimum d'informations[27]. Si tel n'est pas le cas, le consentement obtenu au cours du processus d'inscription ne peut être considéré comme valable au regard du RGPD, le traitement étant dès lors illicite.

28. L'utilisateur est invité à donner son consentement pour différents types de finalités (par exemple, un traitement ultérieur des données à caractère personnel). Le consentement n'étant pas spécifique, il n'est donc pas valable lorsque l'utilisateur ne reçoit pas également des informations claires sur ce à quoi il consent[28]. Comme le prévoit l'article 7, paragraphe 2, du RGPD, le consentement devrait être demandé d'une manière qui le distingue clairement des autres informations, quelle que soit la forme sous laquelle ces informations sont présentées à la personne concernée. Concrètement, lorsque le consentement est demandé par voie électronique, il ne doit pas être inclus dans les conditions générales[29]. Étant donné qu'un nombre croissant d'utilisateurs accèdent aux plateformes de médias sociaux en utilisant l'interface de leurs smartphones pour s'inscrire sur la plateforme, les fournisseurs de médias sociaux doivent accorder une attention particulière à la manière dont ils demandent le consentement, afin de s'assurer qu'il peut être distingué des autres informations. L'utilisateur ne doit pas être confronté à un volume d'informations trop important qui le dissuaderait de lire ces

[25] Lignes directrices 05/2020 de l'EDPB sur le consentement au sens du règlement (UE) 2016/679, version 1.1, adoptées le 4 mai 2020 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_fr.pdf

[26] Voir Cour de justice de l'Union européenne, arrêt du 1er octobre 2019, C-673/17, *Verbraucherzentrale Bundesverband e.V./Planet 49 GmbH*, points 62 et 63.

[27] Lignes directrices 05/2020 sur le consentement, point 64; voir également, ci-dessous, le cas d'utilisation 3a présenté dans la partie 3.3 des présentes lignes directrices.

[28] Voir les lignes directrices 05/2020 sur le consentement, point 68.

[29] Voir les lignes directrices sur la transparence, point 8.

informations. Dans le cas contraire, lorsque l'utilisateur, pour créer un compte, est «tenu» de confirmer qu'il a lu la politique de confidentialité dans son intégralité et qu'il accepte les conditions générales du fournisseur de médias sociaux, y compris toutes les opérations de traitement, cela peut être considéré comme un consentement forcé aux conditions particulières qui y sont énoncées. Si le refus du consentement entraîne un refus du service, il ne saurait être considéré que le consentement est donné librement, de manière distincte et spécifique, comme l'exige le RGPD. Un consentement «associé» à l'acceptation des conditions générales d'un fournisseur de médias sociaux ne saurait être considéré comme «donné librement»[30]. C'est également le cas lorsque le responsable du traitement «subordonne» la fourniture d'un contrat ou d'un service à la demande de consentement, de sorte qu'il traite des données à caractère personnel qui ne sont pas nécessaires à l'exécution du contrat par le responsable du traitement.

29. Si le consentement doit être exprimé par un acte positif de la part de l'utilisateur, l'absence de consentement devrait être considérée comme l'état par défaut, jusqu'à ce que le consentement ait été donné. L'expression du refus de l'utilisateur ne devrait donc nécessiter aucune action de sa part, ou devrait être possible par une action présentant le même degré de simplicité que celle permettant d'exprimer son consentement[31].

ii. Retrait du consentement – Article 7, paragraphe 3, du RGPD

30. En vertu de l'article 7, paragraphe 3, première phrase, du RGPD, les utilisateurs de plateformes de médias sociaux peuvent retirer leur consentement à tout moment. Avant de donner son consentement, l'utilisateur est également informé du droit de retirer son consentement, comme l'exige l'article 7, paragraphe 3, troisième phrase, du RGPD. En particulier, les responsables du traitement doivent démontrer que l'utilisateur a la possibilité de refuser de donner son consentement ou de le retirer sans subir de préjudice. Les utilisateurs de plateformes de médias sociaux qui consentent au traitement de leurs données à caractère personnel par un seul clic, par exemple en cochant une case, pourront retirer leur consentement d'une manière tout aussi simple[32]. Cette exigence souligne que le consentement devrait être une décision réversible, de sorte que la personne concernée conserve un certain degré de contrôle sur le traitement[33]. Le fait de pouvoir retirer facilement son consentement constitue une condition préalable à la validité du consentement au regard de l'article 7, paragraphe 3, quatrième phrase, du RGPD, et devrait être possible sans entraîner la diminution du niveau de service[34]. À titre d'exemple, le consentement ne peut pas être considéré comme valable au regard du RGPD lorsqu'il est obtenu uniquement par un clic, une frappe ou en balayant l'écran, et que le retrait nécessite des étapes supplémentaires[35], est plus difficile à effectuer ou prend davantage de temps.

[30] Voir les lignes directrices 08/2020 sur le ciblage des utilisateurs de médias sociaux, point 57.
[31] Voir considérant 42, cinquième phrase, du RGPD.
[32] Voir les lignes directrices 05/2020 sur le consentement, points 113 et suivants.
[33] Lignes directrices 05/2020 sur le consentement, point 10.
[34] Lignes directrices 05/2020 sur le consentement, point 114.
[35] Voir les lignes directrices 05/2020 sur le consentement, point 114.

c. Interfaces trompeuses

31. Plusieurs dispositions du RGPD portent sur le processus d'inscription. Par conséquent, un certain nombre d'interfaces trompeuses peuvent survenir lorsque les fournisseurs de médias sociaux ne mettent pas en œuvre le RGPD de façon appropriée.

i. Interfaces trompeuses fondées sur le contenu

Surcharge – Incitation répétitive (annexe I, liste de contrôle 4.1.1)

32. Il existe une interface trompeuse de type ***incitation répétitive*** lorsque l'utilisateur est incité à communiquer davantage de données à caractère personnel que ce qui est nécessaire aux fins du traitement ou à accepter une autre utilisation de ses données, en lui demandant à plusieurs reprises de fournir des données supplémentaires ou à consentir à une finalité de traitement. Ces incitations répétitives peuvent survenir sur un ou plusieurs appareils. Il est probable que l'utilisateur, lassé de devoir refuser la demande chaque fois qu'il utilise la plateforme, finisse par céder.

Example 1:

Variante A: lors de la première étape du processus d'inscription, l'utilisateur est tenu de choisir entre différentes options d'enregistrement. Il peut communiquer soit une adresse électronique soit un numéro de téléphone. S'il choisit l'adresse électronique, le fournisseur de médias sociaux tentera malgré tout de le convaincre de communiquer son numéro de téléphone, en indiquant qu'il sera utilisé pour garantir la sécurité du compte et sans proposer d'alternative pour les données qui pourraient être ou ont déjà été fournies par l'utilisateur. Concrètement, plusieurs fenêtres contextuelles apparaissent tout au long du processus d'inscription, dans lesquelles figurent un champ pour le numéro de téléphone ainsi que l'explication suivante: «*Nous utiliserons votre numéro [de téléphone] pour garantir la sécurité du compte*». Bien que l'utilisateur puisse fermer la fenêtre, il est surchargé et finit par céder et communiquer son numéro de téléphone.

Variante B: un autre fournisseur de médias sociaux demande à plusieurs reprises à l'utilisateur de communiquer son numéro de téléphone chaque fois qu'il se connecte à son compte, alors que celui-ci a déjà refusé de le communiquer, que ce soit au cours du processus d'inscription ou lors de la dernière connexion.

33. L'exemple ci-dessus illustre la situation dans laquelle l'utilisateur est constamment invité à fournir des données à caractère personnel spécifiques, telles que son numéro de téléphone. Si, dans la variante A de l'exemple, cette ***incitation répétitive*** intervient à plusieurs reprises au cours du processus d'inscription, la variante B montre que l'utilisateur peut aussi être confronté cette interface trompeuse alors qu'il s'est déjà enregistré. Pour éviter cette interface, il importe d'être particulièrement attentif aux principes de minimisation des données énoncés à l'article 5, paragraphe 1, point c), du RGPD ainsi que, dans des cas tels que celui décrit dans la variante A de l'exemple 1, au principe de limitation des finalités énoncé à l'article 5, paragraphe 1, point b), du RGPD. Par conséquent, lorsque le fournisseur de médias sociaux indique qu'il utilisera le numéro de téléphone «pour garantir la sécurité du compte», il ne doit traiter le numéro de téléphone qu'auxdites fins de sécurité et ne doit pas soumettre ce numéro à un traitement ultérieur qui irait au-delà de cette finalité initiale.

34. Pour respecter le principe de minimisation des données, les fournisseurs de médias sociaux doivent s'abstenir de demander des données supplémentaires telles que le numéro de téléphone, lorsque les données déjà communiquées par l'utilisateur au cours du processus d'inscription sont suffisantes. Par

exemple, pour garantir la sécurité du compte, il est possible de renforcer l'authentification sans le numéro de téléphone en envoyant simplement un code sur les comptes de messagerie de l'utilisateur, ou par plusieurs autres moyens.

35. Les fournisseurs de réseaux sociaux devraient donc recourir à des moyens de sécurité plus faciles à réinitialiser pour l'utilisateur. Par exemple, le fournisseur de médias sociaux peut envoyer à l'utilisateur un numéro d'authentification via un autre canal de communication, tel qu'une application de sécurité, que l'utilisateur aura préalablement installée sur son téléphone portable, mais sans exiger le numéro de téléphone portable de l'utilisateur. L'authentification de l'utilisateur par l'adresse électronique est également moins intrusive que par le numéro de téléphone, car l'utilisateur peut simplement créer une nouvelle adresse électronique spécifiquement pour le processus d'inscription et s'en servir principalement aux fins de la connexion au réseau social. En revanche, un numéro de téléphone n'est pas si facilement interchangeable, car il est très peu probable que l'utilisateur achète une nouvelle carte SIM ou conclue un nouveau contrat de téléphonie aux seules fins de l'authentification.

36. Il convient de garder à l'esprit que, si l'objectif d'une telle demande est de prouver que l'utilisateur est légitimement en possession de l'appareil utilisé pour se connecter au réseau social, cet objectif peut être atteint par plusieurs moyens, le numéro de téléphone n'étant que l'un d'entre eux. Ainsi, un numéro de téléphone ne peut constituer une option pertinente que sur une base volontaire pour l'utilisateur. Enfin, l'utilisateur doit décider s'il souhaite utiliser ce moyen comme facteur d'authentification. Plus précisément, pour une vérification ponctuelle, le numéro de téléphone de l'utilisateur n'est pas nécessaire car l'adresse électronique constitue le point de contact régulier avec l'utilisateur au cours de la procédure d'enregistrement.

37. La pratique illustrée à la variante A de l'exemple 1 peut induire l'utilisateur en erreur et l'amener à fournir ces informations contre son gré, pensant qu'elles sont nécessaires pour activer ou protéger le compte. Or, en réalité, aucune autre solution (par exemple, l'utilisation de l'adresse électronique aux fins de l'activation du compte et de la sécurité) ne lui a jamais été proposée. Dans la variante B de l'exemple 1, l'utilisateur n'est pas informé de la finalité du traitement. Cette variante constitue néanmoins une interface trompeuse de type ***incitation répétitive***, dès lors que le fournisseur de médias sociaux ne tient pas compte du fait que l'utilisateur a déjà refusé de communiquer son numéro de téléphone, et continue de le lui demander. Lorsque l'utilisateur a l'impression que le seul moyen d'éviter cette demande répétée est de communiquer ses données, il est probable qu'il cède.

38. Dans l'exemple suivant, l'utilisateur est encouragé à plusieurs reprises à autoriser la plateforme de médias sociaux à avoir accès à ses contacts:

> **Example 2:** une plateforme de médias sociaux utilise une information ou une icône en forme de point d'interrogation pour inciter l'utilisateur à choisir l'action «facultative» qui lui est alors demandée. Toutefois, au lieu de simplement fournir des informations à l'utilisateur qui s'attend à recevoir de l'aide après avoir cliqué sur ces boutons, la plateforme incite l'utilisateur à accepter l'importation des contacts de son compte de messagerie électronique en affichant à plusieurs reprises une fenêtre contextuelle indiquant «*Allons-y*».

39. En particulier au stade du processus d'inscription, cette ***incitation répétitive*** peut inciter l'utilisateur à accepter la demande de la plateforme afin de terminer la procédure d'enregistrement. Cette interface trompeuse a un effet accru lorsqu'elle est associée à un langage incitatif, comme dans cet exemple, ajoutant ainsi un sentiment d'urgence.

40. Les effets influents de la formulation et des visuels seront abordés plus en détail ci-dessous, dans le cadre de l'examen de l'interface trompeuse de type ***pilotage émotionnel***[36].

Obstruction – Action trompeuse (annexe I, liste de contrôle 4.4.3)

41. Un autre exemple de situation dans laquelle les fournisseurs de médias sociaux demandent le numéro de téléphone de l'utilisateur sans que cela ne soit nécessaire concerne l'utilisation de l'application de la plateforme:

> **Example 3:** lorsqu'il s'inscrit sur une plateforme de médias sociaux par l'intermédiaire d'un navigateur de bureau, l'utilisateur est invité à utiliser également l'application mobile de la plateforme. Au cours de ce qui ressemble à une autre étape du processus d'inscription, il est invité à découvrir l'application. Lorsqu'il clique sur l'icône, croyant être renvoyé vers une boutique d'applications, il est en réalité invité à communiquer son numéro afin de pouvoir recevoir un message contenant un lien vers l'application.

42. Le fait d'indiquer à l'utilisateur qu'il doit donner son numéro de téléphone pour recevoir un lien permettant de télécharger l'application constitue une **action trompeuse,** et ce pour plusieurs raisons: tout d'abord, il existe plusieurs façons pour l'utilisateur d'utiliser une application: par exemple en scannant un code QR, en cliquant sur un lien ou en téléchargeant l'application à partir de la boutique d'applications. Deuxièmement, ces différentes méthodes montrent que rien n'oblige le fournisseur de la plateforme sociale à demander le numéro de téléphone de l'utilisateur. Lorsque l'utilisateur a terminé le processus d'inscription, il doit pouvoir utiliser ses données de connexion (c'est-à-dire généralement une adresse électronique et un mot de passe) pour se connecter quel que soit l'appareil utilisé, qu'il s'agisse d'un ordinateur de bureau, d'un navigateur mobile ou d'une application. Cela est d'autant plus vrai qu'au lieu d'un smartphone, l'utilisateur pourrait souhaiter installer l'application sur sa tablette, qui n'est pas liée à un numéro de téléphone.

Incitation – Pilotage émotionnel (annexe I, liste de contrôle 4.3.1)

43. Dans le cas d'une interface trompeuse de type ***pilotage émotionnel***, la formulation ou les éléments visuels (tels qu'un style, des couleurs, des images ou autres) sont utilisés de manière à transmettre des informations à l'utilisateur sous un jour soit très positif, en faisant en sorte qu'il se sente bien, en sécurité ou récompensé, soit très négatif, en faisant en sorte qu'il se sente angoissé, coupable ou sanctionné. La manière dont les informations sont présentées à l'utilisateur influe sur son état émotionnel d'une manière susceptible de l'amener à agir contre ses intérêts en matière de protection des données. Ces pratiques peuvent être encore plus efficaces si elles se fondent sur des données collectées par la plateforme. Le fait d'influencer les décisions en fournissant des informations biaisées à l'utilisateur peut généralement être considéré comme une pratique déloyale contraire au principe de loyauté du traitement énoncé à l'article 5, paragraphe 1, point a), du RGPD. Cette interface peut survenir tout au long du parcours de l'utilisateur sur une plateforme de médias sociaux. Toutefois, au stade du processus d'inscription, l'effet de pilotage peut être particulièrement marqué, compte tenu de la surcharge d'informations que l'utilisateur peut avoir à traiter en plus des actions nécessaires pour procéder à son enregistrement.

[36] Voir points 43 et suivants du cas d'utilisation 1, ainsi que le récapitulatif des exemples présenté dans la liste de contrôle de l'annexe.

44. À la lumière de ce qui précède, le ***pilotage émotionnel*** au stade de l'enregistrement sur une plateforme de médias sociaux peut avoir un effet encore plus important sur les enfants, les personnes âgées et d'autres groupes (c'est-à-dire qu'ils fournissent davantage de données à caractère personnel parce qu'ils ne comprennent pas les activités de traitement), compte tenu de leur vulnérabilité en tant que personnes concernées[37]. Lorsque les services de plateformes de médias sociaux s'adressent à des enfants ou à d'autres personnes concernées vulnérables, il convient de veiller à ce que le langage utilisé, notamment le ton et le style, soit approprié afin que les utilisateurs vulnérables, en tant que destinataires du message, puissent comprendre aisément les informations fournies[38]. Compte tenu de la vulnérabilité des enfants, des personnes âgées et d'autres personnes concernées, les interfaces trompeuses peuvent inciter ces utilisateurs à communiquer davantage d'informations, car des formulations utilisant l'impératif peuvent leur donner l'impression qu'ils sont obligés de le faire, par exemple pour paraître populaires auprès de leurs pairs ou parce qu'ils pensent qu'il est obligatoire de fournir les données.

45. Lorsqu'un utilisateur de plateformes de médias sociaux est invité à communiquer rapidement ses données, il n'a pas le temps d'«assimiler» les informations qui lui sont fournies, et donc de les comprendre réellement afin de pouvoir prendre une décision éclairée. Le langage incitatif utilisé par les plateformes de médias sociaux pourrait encourager l'utilisateur à fournir ensuite davantage de données que nécessaire, lorsqu'il pense que ce que lui propose la plateforme de médias sociaux est ce que la plupart des utilisateurs feront, et donc la «bonne manière» de procéder.

> **Example 4:** la plateforme de médias sociaux invite l'utilisateur à partager sa géolocalisation par le message suivant: «Salut, vous êtes un loup solitaire? Savez-vous que le partage et la connexion avec les autres contribuent à rendre le monde meilleur? Partagez votre géolocalisation! Laissez-vous inspirer par les lieux et les personnes qui vous entourent!»

46. Au cours du processus d'inscription, l'objectif de l'utilisateur est d'effectuer son enregistrement afin de pouvoir utiliser la plateforme de médias sociaux. Les interfaces trompeuses telles que le **pilotage émotionnel** ont des effets plus importants dans ce contexte. Ils risquent d'être plus marqués au milieu ou vers la fin du processus d'inscription qu'au début, car, le plus souvent, l'utilisateur effectuera toutes les actions nécessaires «dans la précipitation», ou sera davantage susceptible de ressentir un sentiment d'urgence. Dans ce contexte, l'utilisateur risque davantage d'accepter de communiquer toutes les données qu'il est invité à fournir, sans prendre le temps de se demander s'il doit le faire. En ce sens, le langage incitatif utilisé par le fournisseur de médias sociaux peut avoir influé sur la décision instantanée de l'utilisateur, tout comme l'association du langage incitatif à d'autres formes d'emphase, telles que le point d'exclamation, comme l'illustre l'exemple ci-dessous.

> **Example 5:** le fournisseur de médias sociaux utilise des moyens incitatifs afin d'encourager l'utilisateur à partager davantage de données à caractère personnel que ce qui est réellement nécessaire en l'invitant à se décrire: «*Parlez-nous de la personne extraordinaire que vous êtes! Nous avons hâte de savoir, alors racontez-nous sans attendre!*

47. Grâce à cette pratique, les plateformes de médias sociaux obtiennent un profil plus détaillé de leurs utilisateurs. Toutefois, selon le cas, la communication d'un plus grand nombre de données à caractère personnel concernant, par exemple, la personnalité de l'utilisateur n'est pas toujours nécessaire pour utiliser le service lui-même et pourrait donc constituer une violation du principe de minimisation des données énoncé à l'article 5, paragraphe 1, point c), du RGPD. Comme l'illustre l'exemple 5, de telles

[37] Voir également le point 7 ci-dessus.

[38] Voir point 18 des lignes directrices sur la transparence.

techniques ne favorisent pas la libre volonté de l'utilisateur de communiquer ses données, car le langage directif utilisé peut donner à ce dernier l'impression qu'il est obligé de donner une description de lui-même parce qu'il a déjà consacré du temps à l'enregistrement et qu'il souhaite le terminer. Lorsque l'utilisateur est en train d'enregistrer un compte, il est moins susceptible de prendre le temps de réfléchir à la description qu'il donne ou même de se demander s'il souhaite en donner une. Tel est particulièrement le cas lorsque le langage utilisé donne un sentiment d'urgence ou ressemble à un impératif. Si l'utilisateur ressent cette obligation, alors qu'en réalité la communication des données n'est pas obligatoire, cela peut influer sur son «libre arbitre». Cela signifie également que les informations fournies par la plateforme de médias sociaux n'étaient pas claires.

Example 6: la partie du processus d'inscription au cours de laquelle l'utilisateur est invité à télécharger sa photo contient un bouton «?». Lorsque l'utilisateur clique sur ce bouton, le message suivant s'affiche: «*Pas besoin de passer d'abord chez le coiffeur. Choisissez simplement une photo qui vous montre tel que vous êtes*».

48. Même si les phrases de l'exemple 6 ont pour but de motiver l'utilisateur et de simplifier le processus apparemment dans son intérêt (c'est-à-dire qu'il n'est pas nécessaire de fournir une photo officielle pour s'inscrire), de telles pratiques peuvent influer sur la décision finale de l'utilisateur qui avait décidé au départ de ne pas partager de photo sur son compte. Le point d'interrogation est utilisé pour poser des questions et, lorsqu'il est présenté sous la forme d'une icône, l'utilisateur peut s'attendre à trouver des informations utiles en cliquant sur celle-ci. Lorsqu'il ne trouve pas les informations attendues et que, au lieu de cela, il est à nouveau invité à effectuer l'action qu'il hésite à effectuer, le consentement obtenu sans que l'utilisateur n'ait reçu d'informations sur le traitement de sa photo n'est pas valable, puisqu'il ne satisfait pas aux exigences de consentement «éclairé» et «donné librement» énoncées à l'article 7 du RGPD, lu en combinaison avec l'article 4, point 11, du RGPD. Le facteur émotionnel a donc une grande influence sur la légitimité du consentement.

Obstruction – Processus plus long que nécessaire (annexe I, liste de contrôle 4.4.2)

49. Lorsque l'utilisateur tente d'activer un outil de contrôle de la protection des données, mais que le parcours utilisateur est conçu de telle manière qu'il est obligé d'exécuter plus d'actions que nécessaire pour activer des options intrusives relatives aux données, il est en présence d'une interface trompeuse de type ***processus plus long que nécessaire***. Cette interface risque de dissuader l'utilisateur d'activer les outils de contrôle de la protection des données. Au cours du processus d'inscription, elle peut prendre la forme d'une fenêtre («pop-in» ou «pop-up») invitant l'utilisateur à confirmer sa décision lorsqu'il choisit une option restrictive (par exemple, s'il choisit de rendre son profil privé). L'exemple ci-dessous illustre un autre cas où le processus d'inscription est ***plus long que nécessaire***.

Example 7: au cours du processus d'inscription, l'utilisateur qui clique sur les boutons «passer» pour éviter de saisir certaines données voit s'afficher une fenêtre contextuelle demandant «*Êtes-vous sûr?*». En remettant en question sa décision et, partant, en le faisant douter, le fournisseur de médias sociaux incite l'utilisateur à reconsidérer sa décision et à divulguer ces données, par exemple son genre, la liste de ses contacts ou une photo. En revanche, l'utilisateur qui choisit de saisir directement ces données ne voit s'afficher aucun message l'invitant à reconsidérer son choix.

Dans ce cas précis, le fait de demander à l'utilisateur de confirmer qu'il ne souhaite pas remplir un champ de données peut l'inciter à revenir sur sa décision initiale et à fournir les données demandées. C'est notamment le cas pour les utilisateurs qui ne connaissent pas bien les fonctions

de la plateforme de médias sociaux. Cette interface trompeuse de type ***processus plus long que nécessaire*** tente d'influencer les décisions de l'utilisateur en les freinant et en remettant en question son choix initial, en plus de prolonger inutilement le processus d'inscription, ce qui constitue une violation du principe de loyauté énoncé à l'article 5, paragraphe 1, point a), du RGPD. L'exemple montre que l'interface trompeuse peut amener l'utilisateur à divulguer (davantage) de données à caractère personnel qu'il ne l'avait décidé au départ. Il décrit un déséquilibre dans le traitement des utilisateurs, selon qu'ils divulguent immédiatement des données à caractère personnel ou non: seuls ceux qui refusent de divulguer les données sont invités à confirmer leur choix, tandis que les utilisateurs qui les divulguent ne sont pas invités à le faire. Cela constitue une violation du principe de loyauté énoncé à l'article 5, paragraphe 1, point a), du RGPD à l'égard des utilisateurs qui ne souhaitent pas divulguer ces données à caractère personnel.

ii. Interfaces trompeuses fondées sur le processus de navigation

Incitation – Caché au grand jour (annexe I, liste de contrôle 4.3.2)

50. Conformément au principe de transparence, les personnes concernées doivent recevoir des informations claires leur permettant de comprendre comment leurs données à caractère personnel sont traitées et comment elles peuvent les contrôler. En outre, ces informations doivent être facilement perceptibles par les personnes concernées. Or, les informations relatives à la protection des données, en particulier les liens, sont souvent présentées de telle manière qu'elles échappent facilement à l'utilisateur. Ces pratiques de ***cacher au grand jour*** consistent à utiliser, pour les informations ou les outils de contrôle de la protection des données, un style visuel qui empêche l'utilisateur de voir les options avantageuses en matière de protection des données et le pousse vers des options moins restrictives et donc plus intrusives.

51. L'utilisation d'une police de caractères de petite taille ou d'une couleur qui n'est pas suffisamment contrastée pour offrir une lisibilité suffisante (par exemple, un texte de couleur gris clair sur fond blanc) peut avoir un effet négatif sur l'utilisateur: le texte étant moins visible, il ne le remarque pas ou a du mal à le lire. Tel est notamment le cas lorsqu'un ou plusieurs éléments accrocheurs sont placés à côté des informations obligatoires relatives à la protection des données. Ces techniques d'interface induisent l'utilisateur en erreur et rendent la recherche d'informations relatives à la protection de ses données plus fastidieuse et chronophage, car il faut davantage de temps et de minutie pour repérer les informations utiles.

> **Example 8:** tout de suite après l'enregistrement, l'utilisateur ne peut accéder aux informations relatives à la protection des données qu'en ouvrant le menu général de la plateforme de médias sociaux et en parcourant la section du sous-menu où figure un lien vers les «*paramètres de protection de la vie privée et des données*». Sur cette page, aucun lien vers la politique de confidentialité n'est visible à première vue. L'utilisateur doit remarquer, dans un coin de la page, une minuscule icône indiquant la politique de confidentialité, ce qui signifie qu'il peut difficilement voir où se trouvent les informations relatives à la protection des données.

52. Il convient de faire remarquer que, même lorsque les fournisseurs de médias sociaux fournissent toutes les informations qu'ils sont tenus de fournir aux personnes concernées en vertu des articles 13 et 14 du RGPD, la manière dont ces informations sont présentées peut néanmoins violer les exigences générales de transparence prévues à l'article 12, paragraphe 1, du RGPD. Lorsque les informations sont

cachées au grand jour et donc susceptibles d'échapper à l'utilisateur, cela entraîne une confusion ou une désorientation et les informations ne peuvent être considérées comme compréhensibles et aisément accessibles, contrairement à ce qu'exige l'article 12, paragraphe 1, du RGPD.

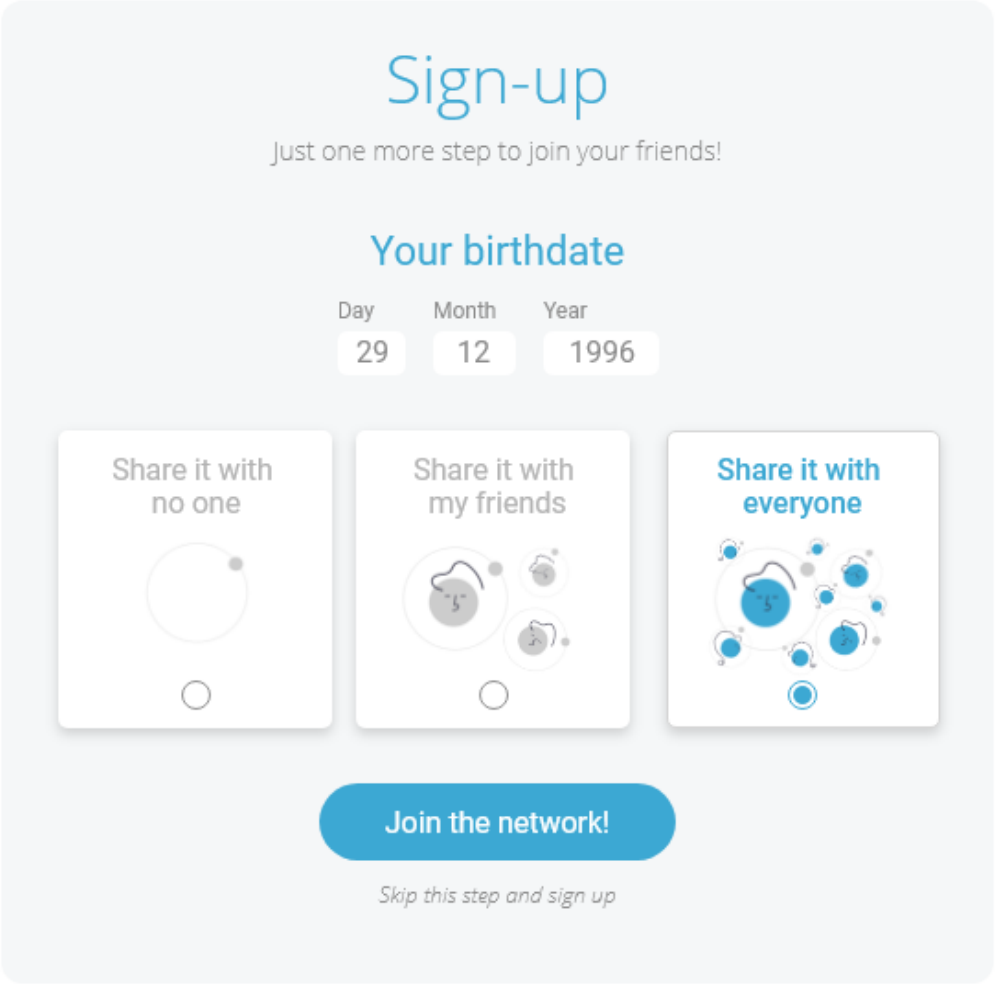
53. Si l'exemple ci-dessus illustre l'interface trompeuse après l'achèvement du processus d'inscription, cette interface peut également survenir au cours de ce processus, comme le montrera l'exemple ci-dessous, qui combine les interfaces trompeuses ***caché au grand jour*** et ***confort trompeur***.

Inattention – Confort trompeur (annexe I, liste de contrôle 4.2.1)

54. Les fournisseurs de médias sociaux doivent également être attentifs au principe de protection des données par défaut. Lorsque les paramètres des données sont prédéfinis, l'utilisateur est soumis à un niveau spécifique de protection des données, déterminé par défaut par le fournisseur et non par l'utilisateur lui-même. En outre, l'utilisateur n'a pas toujours immédiatement la possibilité de modifier les paramètres et d'en choisir de plus stricts, conformes à la protection des données. Le respect du RGPD à cet égard ne signifie pas que toutes les options doivent être parfaitement identiques. Toutefois, si le fournisseur de médias sociaux met en évidence l'une des options, attirant ainsi l'attention de l'utilisateur sur celle-ci, il doit choisir la plus restrictive en ce qui concerne les données à caractère personnel, afin de se conformer, notamment, au principe de minimisation des données énoncé à l'article 5, paragraphe 1, point c), du RGPD.

55. Lorsque les fonctionnalités et les options les plus intrusives pour les données sont activées par défaut, il s'agit d'une interface trompeuse de type ***confort trompeur***. En raison de l'effet «par défaut» qui pousse l'utilisateur à conserver une option par défaut, il est peu probable que celui-ci modifie cette option, même s'il en a la possibilité. Cette pratique est fréquente dans les processus d'inscription, comme l'illustre l'exemple 9 ci-dessous, car il s'agit d'un moyen efficace d'activer des options intrusives en matière de données, que l'utilisateur refuserait probablement dans d'autres circonstances. De telles interfaces trompeuses sont contraires au principe de protection des données par défaut énoncé à l'article 25, paragraphe 2, du RGPD, en particulier lorsqu'elles ont une incidence sur la collecte de données à caractère personnel, l'étendue du traitement, la durée de stockage des données et l'accessibilité des données[39].

[39] Voir également la décision finale de l'autorité irlandaise chargée de la protection des données concernant Instagram (Meta Platforms Ireland Limited) faisant suite à la décision contraignante en matière de litiges de l'EDPB du 28 juillet 2022, point 446, à l'adresse suivante:https://edpb.europa.eu/news/news/2022/record-fine-instagram-following-edpb-intervention_fr



Example 9: dans cet exemple, lorsque l'utilisateur saisit sa date de naissance, il est invité à choisir avec qui il accepte de partager cette information. Alors que des options moins intrusives sont disponibles, c'est l'option «*partager avec tout le monde*» qui est sélectionnée par défaut, ce qui signifie que tout le monde (les utilisateurs enregistrés ainsi que tous les internautes) pourra voir la date de naissance de l'utilisateur.

56. L'exemple 9 illustre une interface trompeuse de type ***confort trompeur***, car ce n'est pas l'option offrant le niveau le plus élevé de protection des données qui est sélectionnée, et donc activée, par défaut. En outre, l'effet «par défaut» de cette interface pousse l'utilisateur à conserver la sélection par défaut, c'est-à-dire à ne pas prendre le temps d'examiner les autres options à ce stade et à ne pas revenir en arrière pour modifier le paramètre à un stade ultérieur. L'interface trompeuse de type ***caché au grand jour*** est également utilisée dans cette interface. En effet, il n'est pas obligatoire d'indiquer sa date de naissance, car l'utilisateur peut passer cette étape de l'inscription en cliquant sur le lien «*Passer cette étape et m'inscrire*» disponible sous le bouton «*Rejoindre le réseau!*». Le fait que le champ de la date de naissance et le bouton de confirmation soient aussi visibles est susceptible d'inciter l'utilisateur à saisir sa date de naissance et à la communiquer au réseau social parce qu'il ne remarque pas l'option lui permettant de ne pas partager cette information. Cet effet serait encore renforcé si des cercles animés apparaissaient à côté du champ et du bouton, attirant fortement l'attention de l'utilisateur.

57. Le respect du principe de protection des données dès la conception et de protection des données par défaut ne signifie pas que toutes les options proposées doivent avoir une apparence identique. Toutefois, si les responsables du traitement décident de mettre en avant une option plus qu'une autre, il doit s'agir de l'option la plus restrictive en ce qui concerne le traitement des données.

58. En plus de pousser l'utilisateur à conserver une option qui ne correspond pas nécessairement à ses préférences, les fournisseurs de médias sociaux pourraient ne pas inviter l'utilisateur à vérifier ou à modifier ses paramètres de protection des données en fonction de ses préférences après avoir terminé le processus d'inscription. En outre, la modification de ces paramètres par défaut pourrait nécessiter plusieurs étapes. Lorsque l'utilisateur n'est en aucune manière incité à vérifier ou à modifier ses paramètres de protection des données ou n'est pas orienté de manière claire vers des informations à ce sujet, le niveau de protection de ses données dépendra de son initiative personnelle. Pour faciliter le contrôle de ses données par l'utilisateur, il est possible d'utiliser des tableaux de bord sur la protection de la vie privée, conçus pour centraliser et faciliter ce contrôle.

59. Il importe de garder à l'esprit que l'absence de protection des données dès la conception et de protection des données par défaut, combinée à l'effet «par défaut» susmentionné, peut avoir des conséquences préjudiciables pour les personnes concernées, y compris en ce qui concerne leur cybersécurité. L'affichage public de données à caractère personnel, telles que la date de naissance, qui sont utilisées à des fins de vérification par d'autres services en ligne pourrait permettre à des criminels d'accéder plus facilement aux comptes d'achat, aux comptes bancaires et à d'autres comptes de l'utilisateur. Une autre conséquence préjudiciable concerne les possibilités de contact sur la plateforme de médias sociaux: si l'option sélectionnée par défaut pour l'envoi de demandes de contact ou de messages à l'utilisateur est l'option «tout le monde», il existe un risque d'abus sexuels d'enfants sur internet et de fraude, en particulier pour les groupes vulnérables.

60. Enfin, lorsque la technique du ***confort trompeur*** est appliquée pour obtenir le consentement, ce qui reviendrait à considérer que l'utilisateur donne son consentement par défaut, par exemple en utilisant une case cochée par défaut ou en considérant que l'inactivité a valeur d'approbation, les conditions du consentement énoncées à l'article 4, point 11, du RGPD ne sont pas satisfaites et le traitement doit être considéré comme illicite au regard de l'article 5, paragraphe 1, point a), et de l'article 6, paragraphe 1, point a), du RGPD.

Obstruction – Impasse (annexe I, liste de contrôle 4.4.1)

61. Il convient de souligner que l'étape du processus d'inscription est un moment déterminant pour l'information de l'utilisateur. Si l'utilisateur recherche des informations et ne peut les trouver parce qu'aucun lien de redirection ne lui est proposé ou ne fonctionne, il s'agit d'une interface de type ***impasse***, car l'utilisateur n'a pas les moyens d'atteindre cet objectif.

> **Example 10:** aucun lien vers des informations relatives à la protection des données n'est proposé à l'utilisateur une fois qu'il a entamé le processus d'inscription. L'utilisateur ne peut pas trouver ces informations car elles ne figurent nulle part dans l'interface d'inscription, pas même dans le pied de page.

62. Dans la pratique, cet exemple signifie que l'utilisateur ne pourra qu'interrompre l'enregistrement et revenir à la page d'accueil si celle-ci contient un lien vers la déclaration de confidentialité, ou terminer l'enregistrement, se connecter à la plateforme de médias sociaux et seulement alors avoir accès aux informations relatives à la protection des données. Cette technique viole le principe de transparence

et de d'accès aisé aux informations qui doivent être fournies aux personnes concernées, comme l'exige l'article 12, paragraphe 1, du RGPD. Elle ne satisfait pas non plus aux exigences de l'article 13, paragraphes 1 et 2 du RGPD, dès lors qu'aucune information n'est fournie ni accessible au moment où les données à caractère personnel sont obtenues.

63. L'interface de type ***impasse*** peut également prendre une autre forme lorsque durant le processus d'inscription, l'utilisateur se voit proposer une action ou une option liée à la protection des données qu'il ne peut pas retrouver plus tard, lors de l'utilisation du service.

> **Example 11:** au cours du processus d'inscription, l'utilisateur peut consentir au traitement de ses données à caractère personnel à des fins publicitaires, et il est informé qu'il peut modifier son choix à tout moment après s'être enregistré sur le réseau social en consultant la politique de confidentialité. Toutefois, une fois que l'utilisateur a terminé la procédure d'enregistrement et qu'il consulte la politique de confidentialité, il ne trouve aucun moyen de retirer son consentement à ce traitement, ni aucune indication sur la manière de le faire.

64. Dans cet exemple spécifique, l'utilisateur n'a aucun moyen de retirer son consentement une fois qu'il s'est inscrit. Dans ce cas précis, l'interface trompeuse de type ***impasse*** viole le droit des personnes concernées de retirer leur consentement à tout moment, et de manière aussi simple qu'elles l'ont donné, comme l'exige l'article 7, paragraphe 3, première et quatrième phrases, du RGPD.

65. Enfin, le fait d'orienter l'utilisateur vers un lien supposé le mener vers des pages en rapport avec la protection des données, telles que des paramètres ou des informations relatives à la protection des données, constitue également un exemple d'interface de type ***impasse*** si le lien ne fonctionne pas et qu'aucun autre lien n'est mis à la disposition de l'utilisateur pour l'aider à trouver ce qu'il recherche. De cette façon, l'utilisateur ne peut pas rechercher les informations utiles, et aucune explication ne lui est fournie, comme la raison de cette situation (par exemple, des problèmes techniques). Dans un tel cas, les mêmes problèmes que ceux décrits au point 58 se posent en ce qui concerne la transparence et l'accès aisé aux informations.

d. Bonnes pratiques

Afin de concevoir des interfaces utilisateur qui facilitent la mise en œuvre effective du RGPD, l'EDPB recommande de mettre en œuvre les bonnes pratiques suivantes au cours du processus d'inscription:

> **Raccourcis**: des liens vers des informations, des actions ou des paramètres pouvant aider concrètement l'utilisateur à gérer ses données et ses paramètres de protection des données devraient être proposés partout où il est confronté à des informations ou à des expériences connexes (*par exemple, des liens redirigeant vers les parties pertinentes de la politique de confidentialité*).
>
> **Coordonnées**: l'adresse de contact de la société à laquelle l'utilisateur peut envoyer des demandes concernant la protection des données devrait être clairement indiquée dans la politique de confidentialité. Elle devrait figurer dans une section où l'utilisateur peut s'attendre à la trouver, par exemple une section concernant l'identité du responsable du traitement des données, une section relative aux droits ou une section de contact.
>
> **Contacter l'autorité de contrôle**: indiquer l'identité précise de l'autorité de contrôle et insérer un lien vers son site internet ou vers la page internet consacrée à l'introduction d'une réclamation. Ces informations devraient figurer dans une section où l'utilisateur peut s'attendre à les trouver, par exemple une section relative aux droits.

Aperçu de la politique de confidentialité: au début ou en haut de la politique de confidentialité, insérer une table des matières (dépliable) avec des titres et des sous-titres indiquant les différents passages de la déclaration de confidentialité. Les noms des différents passages indiquent clairement à l'utilisateur le contenu exact et lui permettent de repérer et d'atteindre rapidement la section qu'il recherche.

Détection des changements et comparaison: lorsque des modifications sont apportées à la déclaration de confidentialité, donner accès aux versions antérieures, en indiquant la date de leur publication et en mettant en évidence les changements effectués.

Formulation cohérente: il convient d'utiliser une formulation et une définition identiques pour le même dispositif de protection des données sur l'ensemble du site internet. La formulation utilisée dans la politique de confidentialité devrait être identique à celle utilisée sur le reste de la plateforme.

Fournir des définitions: en cas d'utilisation de mots ou de jargon non familiers ou techniques, fournir une définition en des termes simples aidera l'utilisateur à comprendre les informations qui lui sont communiquées. La définition peut être donnée directement dans le texte, lorsque l'utilisateur passe sur le mot, ou figurer dans un glossaire.

Mettre en évidence les éléments relatifs à la protection des données: rendre visuellement frappants les éléments ou actions liés à la protection des données dans une interface qui ne concerne pas directement ce sujet. Par exemple, lors de l'affichage d'un message public sur la plateforme, les outils permettant de contrôler l'association de la géolocalisation devraient être directement disponibles et clairement visibles.

Intégration de la protection des données: aussitôt après la création d'un compte, inclure des points relatifs à la protection des données dans l'expérience d'accueil du fournisseur de médias sociaux pour que l'utilisateur découvre et définisse ses préférences sans difficulté. Par exemple, l'inviter à définir ses préférences en matière de protection des données après avoir ajouté son premier ami ou partagé son premier post.

Utilisation d'exemples: outre les informations obligatoires indiquant de façon claire et précise la finalité du traitement, des exemples peuvent être utilisés pour illustrer un traitement de données spécifique et le rendre ainsi plus concret pour l'utilisateur.

Informations contextuelles: en plus d'une politique de confidentialité exhaustive, apporter de brèves informations au moment le plus opportun pour que l'utilisateur dispose en permanence d'informations spécifiques sur la manière dont ses données sont traitées.

3.2 S'informer sur les réseaux sociaux

Cas d'utilisation n° 2a: une déclaration de confidentialité à plusieurs niveaux

a. **Description du contexte**

66. Comme l'EDPB l'a déjà souligné dans les lignes directrices sur la transparence, le principe de transparence est très étroitement lié au principe du traitement loyal des données à caractère personnel[40]. Toutefois, les informations sur le traitement des données à caractère personnel permettent également aux responsables du traitement de réfléchir à leurs propres actions, de rendre le traitement des données plus compréhensible pour les personnes concernées et, en fin de compte, de donner aux personnes concernées les moyens d'avoir le contrôle de leurs données, notamment en

[40] Lignes directrices sur la transparence, p. 4 et 5.

exerçant leurs droits. Le nivellement des capacités des personnes concernées qui en résulte donne lieu à un système de traitement loyal des données à caractère personnel. Cependant, l'augmentation de la quantité d'informations ne va pas nécessairement de pair avec l'amélioration de leur qualité. Une quantité excessive d'informations dénuées de pertinence ou prêtant à confusion peut masquer des points de contenu importants ou réduire la probabilité de les trouver. Il est donc primordial, dans ce domaine, de trouver un juste équilibre entre le contenu et une présentation compréhensible. À défaut, des interfaces trompeuses peuvent survenir.

b. **Dispositions juridiques pertinentes**

67. Les liens décrits ci-dessus deviennent clairs au vu de l'article 5 du RGPD. La transparence et la loyauté sont déjà systématiquement mentionnées côte à côte à l'article 5, paragraphe 1, point a), du RGPD, puisque l'un détermine l'autre. Le fait que la transparence doive être à la fois externe et interne ressort également clairement de l'exigence de responsabilité prévue à l'article 5, paragraphe 2, du RGPD. La partie la plus importante de la transparence interne est l'obligation de tenir un registre des activités de traitement conformément à l'article 30 du RGPD. Pour assurer la transparence externe, les fournisseurs de médias sociaux peuvent, entre autres moyens d'information, fournir à l'utilisateur une déclaration de confidentialité à plusieurs niveaux[41]. Cette nécessité de fournir des informations compréhensibles et d'assurer un traitement loyal découle également des exigences de l'article 12, paragraphe 1, du RGPD, qui dispose que toute information visée aux articles 13 et 14 du RGPD doit être fournie d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples. Par conséquent, le contenu de l'information doit être mis à disposition de l'utilisateur sans obstacles. Si les exigences de l'article 12 du RGPD ne sont pas satisfaites, il n'existe pas d'informations valables au sens des articles 13 et 14 du RGPD. Dès lors, aux fins d'un contrôle efficace, les responsables du traitement et les sous-traitants peuvent être tenus de rendre des comptes, garantissant ainsi l'efficacité des exigences du RGPD dans la pratique.

c. Interfaces trompeuses

i. Interfaces trompeuses fondées sur le contenu

68. En ce qui concerne ce cas d'utilisation, les interfaces trompeuses fondées sur le contenu trouvent leurs limites à l'article 12, paragraphe 1, du RGPD, qui exige que les informations soient fournies d'une façon précise et compréhensible, en des termes clairs et simples.

Brouillage – Informations contradictoires (annexe I, liste de contrôle 4.6.2)

69. L'un des cas de brouillage les plus flagrants est celui dans lequel des ***informations contradictoires*** sont fournies, laissant l'utilisateur dans l'incertitude quant à ce qu'il doit faire et aux conséquences de ses actions, et l'incitant donc à ne rien faire ou à conserver les paramètres par défaut.

70. Les infractions dans ce domaine, telles que la violation de l'article 12, paragraphe 1, du RGPD, peuvent être amplifiées par d'autres effets tels que le ***pilotage émotionnel***. Les textes, images et couleurs incitatifs, ainsi que les publicités attractives sont en principe autorisés. Ils sont toutefois susceptibles d'accroître l'effet des interfaces trompeuses, notamment le traitement déloyal au sens de l'article 5, paragraphe 1, point a), du RGPD.

[41] Voir cas d'utilisation n° 2a dans la section 3.2 ci-dessous.

Sharing your information

On our platform you can **share everything and anything**! The more you share, the **more exciting** your **experience** will be! And at any time you can set your preference on the visibility of the information you share on our platform.

For example, you can decide if you want to **share your geolocation** or who will be able to read your posts.

If you **change the publicity of your information** once it is posted online, you will lose visibility and some people might not be able to see it anymore.

Example 12: dans cet exemple, les informations relatives au partage des données donnent une vision très positive du traitement en soulignant les avantages liés au partage du plus grand nombre de données possible. Ce ***pilotage émotionnel,*** associé à l'illustration représentant un mignon petit animal jouant avec une balle, peut donner à l'utilisateur une impression de sécurité et de confort quant aux risques potentiels liés au partage de certaines informations sur la plateforme. Par ailleurs, les informations fournies sur la manière de contrôler la publicité de ses données ne sont pas claires. Tout d'abord, il est indiqué que l'utilisateur peut définir ses préférences de partage quand il le souhaite. Cependant, la dernière phrase indique que cela n'est pas possible lorsque l'utilisateur a déjà publié quelque chose sur la plateforme. Ces éléments d'***informations contradictoires*** laissent l'utilisateur dans l'incertitude quant à la manière de contrôler la publicité de ses données.

Inconstance – Manque de hiérarchie (annexe I, liste de contrôle 4.5.1)

71. Des effets semblables à ceux des ***informations contradictoires*** et du ***pilotage émotionnel*** peuvent survenir si la présentation des informations ne suit pas un système interne ou une hiérarchie. On observe un ***manque de hiérarchie*** dans les informations relatives à la protection des données lorsque ces informations apparaissent à plusieurs reprises et sont présentées de plusieurs manières différentes. L'utilisateur risque d'être désorienté face à cette redondance et de ne pas pouvoir comprendre pleinement comment ses données sont traitées et comment exercer un contrôle sur celles-ci. Dans une telle architecture, les informations sont difficiles à comprendre en raison du manque d'accès à une vue d'ensemble. Dans les cas comme celui décrit dans l'exemple suivant, cette absence de hiérarchie constitue une violation des exigences relatives aux informations compréhensibles et aisément accessibles prévues à l'article 12, paragraphe 1, du RGPD.

Example 13: les informations relatives aux droits des personnes concernées sont disséminées dans différentes sections de la déclaration de confidentialité. Bien que certains de ces droits soient expliqués dans la section «*Vos options*», le droit d'introduire une réclamation et l'adresse de contact précise ne sont indiqués qu'après plusieurs sections et niveaux traitant de différents thèmes. La déclaration de confidentialité omet donc en partie de mentionner les coordonnées de contact à des stades où il serait souhaitable qu'elles y figurent.

72. Un ***manque de hiérarchie*** peut également exister lorsque les informations données sont structurées de telle manière qu'il est difficile pour l'utilisateur de s'orienter, comme le montre l'exemple suivant.

Example 14: la politique de confidentialité n'est pas divisée en plusieurs sections contenant chacune des titres et du texte. Elle fait plus de 70 pages, mais il n'y a pas de menu de

navigation sur le côté ou en haut de la page pour permettre à l'utilisateur d'atteindre facilement la section qu'il recherche. L'explication de l'expression «*données de création*» créée par le fournisseur lui-même figure dans une note de bas de page, à la page 67.

Brouillage – Formulations ou informations ambiguës (annexe I, liste de contrôle 4.6.3)

73. Même si le choix des mots n'est pas ouvertement contradictoire, l'utilisation de termes ambigus et vagues dans les informations fournies à l'utilisateur peut poser problème. En présence de telles informations, l'utilisateur risque de ne pas savoir comment ses données seront traitées ni comment exercer un certain contrôle sur ces données. Si l'on peut supposer que l'utilisateur moyen ne comprendrait pas le véritable message des informations sans connaissances particulières, les conditions de l'article 12, paragraphe 1, du RGPD ne sont pas satisfaites. Par extension, l'utilisation de ***formulations ou d'informations ambiguës*** peut aller à l'encontre du principe de loyauté énoncé à l'article 5, paragraphe 1, point a), du RGPD, dès lors que les informations ne peuvent pas être considérées comme transparentes, puisqu'elles mettent les personnes concernées dans l'incapacité de comprendre le traitement de leurs données à caractère personnel et d'exercer leurs droits.

Example 15: une déclaration de confidentialité décrit une partie d'un traitement de façon vague et imprécise, comme dans la phrase suivante: «*Vos données pourraient être utilisées pour améliorer nos services*». En outre, le droit d'accès aux données à caractère personnel s'applique au traitement comme l'exige l'article 15, paragraphe 1, du RGPD, mais il est mentionné d'une telle manière que l'utilisateur ne sait pas exactement à quoi il peut avoir accès: *«Vous pouvez consulter une partie de vos informations dans votre compte et en examinant ce que vous avez publié sur la plateforme».*

74. Dans l'exemple, l'utilisation du conditionnel («*pourraient*») ne permet pas à l'utilisateur de savoir avec certitude si ses données seront utilisées ou non pour le traitement. Le terme «*services*» est probablement trop général pour être considéré comme «clair». Qui plus est, la manière dont les données seront traitées pour améliorer les services n'est pas claire. L'EDPB rappelle que l'utilisation du conditionnel ou d'une formulation vague ne constitue pas des «termes clairs et simples», comme l'exige l'article 12, paragraphe 1, première phrase, du RGPD, et n'est autorisée que si les responsables du traitement sont en mesure de démontrer que cela ne porte pas atteinte à la loyauté du traitement[42].

Inconstance – Discontinuité linguistique (annexe I, liste de contrôle 4.5.4)

75. Lorsque des services en ligne sont proposés à destination des résidents de certains États membres, les avis sur la protection de la vie privée devraient également être proposés dans les langues de ces États[43]. Dans ce contexte, il est important que le choix d'une langue particulière puisse également être effectué manuellement et qu'il soit appliqué de manière continue, sans interruption. Si ces critères ne sont pas satisfaits, les personnes concernées sont confrontées à une ***discontinuité linguistique*** qui les empêche de comprendre les informations relatives à la protection des données. L'utilisateur est confronté à cette interface trompeuse lorsque les informations relatives à la protection des données ne sont pas communiquées dans la langue officielle du pays où il vit, alors que le service est fourni dans cette langue. Si l'utilisateur ne maîtrise pas la langue dans laquelle les informations relatives à la protection

[42] Voir les lignes directrices sur la transparence, point 12, y compris les «exemples de mauvaises pratiques», et le point 13.
[43] Voir les lignes directrices sur la transparence, point 13 et note de bas de page 15.

des données lui sont communiquées, il ne pourra pas les lire aisément et ne saura donc pas comment ses données à caractère personnel sont traitées. Il convient de faire remarquer que la ***discontinuité linguistique*** peut désorienter l'utilisateur et créer un environnement contextuel qu'il ne sait pas comment utiliser. Cette interface trompeuse peut prendre différentes formes, comme le montreront les présentes lignes directrices.

Example 16:

Variante A: la plateforme de médias sociaux est disponible en croate, qui est la langue choisie par l'utilisateur (ou en espagnol, langue du pays dans lequel il se trouve), tandis que toutes les informations relatives à la protection des données, ou certaines d'entre elles, ne sont fournies qu'en anglais.

Variante B: chaque fois que l'utilisateur consulte certaines pages, comme la page d'aide, celles-ci basculent automatiquement dans la langue du pays dans lequel il se trouve, même s'il a préalablement sélectionné une autre langue.

76. La variante A illustre le cas dans lequel aucune information n'est disponible dans une langue apparemment maîtrisée par la personne concernée. Cela signifie qu'elle ne peut pas lire les informations et, par conséquent, qu'elle ne peut pas comprendre comment ses données à caractère personnel sont traitées. Les informations ne peuvent pas être considérées comme compréhensibles comme l'exige l'article 12, paragraphe 1, du RGPD. Dès lors que les informations relatives à la protection des données ne sont pas fournies d'une façon compréhensible, les informations requises au titre des articles 13 et 14 du RGPD ne sauraient être considérées comme ayant été fournies aux personnes concernées.

77. La variante B décrit un cas dans lequel les pages contenant les informations relatives à la protection des données sont présentées par défaut dans la langue du pays de résidence de l'utilisateur, même si celui-ci a clairement choisi sa langue. Cela signifie que l'utilisateur doit réinitialiser ses préférences linguistiques chaque fois qu'il accède à une page d'information sur la protection des données. Cette pratique peut être considérée comme déloyale à l'égard des personnes concernées et pourrait contribuer à une violation du principe de loyauté énoncé à l'article 5, paragraphe 1, point a), du RGPD.

ii. Interfaces trompeuses fondées sur le processus de navigation

78. Dans certains cas, les fournisseurs de médias sociaux ont recours à des pratiques spécifiques pour présenter leurs paramètres de protection des données. Au cours du processus d'inscription, l'utilisateur reçoit une grande quantité d'informations et se voit proposer différents paramètres relatifs à la protection des données. Afin de s'assurer que l'utilisateur peut localiser ces paramètres et les modifier à tout moment lorsqu'il utilise la plateforme, il convient de faire en sorte qu'ils soient aisément accessibles et associés à des informations utiles permettant à l'utilisateur de prendre une décision éclairée. Le critère «aisément accessible» signifie que la personne concernée ne devrait pas avoir à rechercher les informations. En ce qui concerne les politiques de confidentialité, le groupe de travail «Article 29» a déjà indiqué que les textes ou liens dont la mise en page ou le choix de couleur les rend moins visibles ou difficiles à trouver sur une page web ne sont pas considérés comme aisément accessibles[44].

[44] Voir les lignes directrices sur la transparence, point 11.

Surcharge – Labyrinthe (annexe I, liste de contrôle 4.1.2)

79. Selon les lignes directrices sur la transparence, la déclaration de confidentialité devrait être aisément accessible, c'est-à-dire en un seul clic sur les sites internet[45]. Le fait d'utiliser l'approche à plusieurs niveaux peut aider à présenter la déclaration de confidentialité de façon plus claire, au sens de l'article 12, paragraphe 1, du RGPD[46]. Toutefois, cette approche ne devrait pas avoir pour effet de rendre inutilement difficile l'exercice de fonctions ou de droits importants en proposant une politique de confidentialité complexe, composée d'innombrables niveaux, qui donnerait lieu à une interface trompeuse de type ***labyrinthe***. Cette interface survient lorsqu'une information ou un outil de contrôle de la protection des données est particulièrement difficile à trouver, l'utilisateur étant contraint de naviguer sur de nombreuses pages sans disposer d'une vue d'ensemble complète et exhaustive. Il est donc probable, dans ces conditions, que l'utilisateur passe à côté des informations/paramètres utiles ou qu'il renonce à les chercher. La structure à plusieurs niveaux a pour but de faciliter la lisibilité et de donner aux personnes concernées des informations sur la manière d'exercer leurs droits, et non de les rendre plus difficiles. Il est essentiel de veiller à ce que l'utilisateur puisse facilement suivre les explications.

80. À cet égard, la meilleure solution pour l'utilisateur ne réside pas dans une approche uniforme et dépend de nombreux critères, tels que le type d'utilisateurs de la plateforme ou le type général de conception de l'application. Dans la mesure du possible, il convient de tester l'approche à plusieurs niveaux mise en œuvre auprès des utilisateurs et de leur demander leur avis afin d'en évaluer l'efficacité. C'est pourquoi il n'est pas possible de quantifier concrètement le nombre maximal de niveaux d'information autorisés. Il convient donc toujours de déterminer au cas par cas si le nombre de niveaux utilisés est trop élevé et si, de ce fait, on se trouve en présence d'interfaces trompeuses. Toutefois, plus ce nombre est élevé, plus on peut supposer que l'utilisateur sera découragé ou induit en erreur. Un nombre élevé de niveaux ne sera approprié que dans des cas particuliers où il n'est pas facile de fournir des informations complexes de manière exhaustive. Dans le même temps, l'approche à plusieurs niveaux ne doit pas être utilisée à mauvais escient pour dissimuler des informations dans des niveaux plus profonds ou en ajoutant des niveaux inutiles.

81. Toutefois, cet aspect doit être apprécié différemment en ce qui concerne l'exercice des droits des utilisateurs. Le RGPD exige que l'exercice de ces droits soit toujours accordé. Ce cadre détermine la présentation des informations sur les fonctions connexes et l'exercice des droits. Lorsque l'utilisateur souhaite exercer ses droits, le nombre d'étapes du processus devrait être réduit au minimum. Ainsi, l'utilisateur devrait pouvoir accéder aussi directement que possible à la fonction qui lui permet d'exercer ses droits. Dans la plupart des cas, le fait de devoir naviguer à travers de nombreux niveaux d'information avant de pouvoir effectivement exercer ses droits au moyen de fonctions pourrait dissuader l'utilisateur d'exercer ces droits. Si le fournisseur de médias sociaux prévoit de nombreuses étapes, il devrait être en mesure de démontrer que cela profite à l'utilisateur en tant que personne concernée au sens du RGPD. Outre l'explication des droits conférés à la personne concernée dans la déclaration de confidentialité, comme l'exige l'article 13, paragraphe 2, points b), c) et d), du RGPD, l'utilisateur devrait également avoir accès à l'exercice des droits indépendamment de ces informations. Par exemple, il devrait aussi pouvoir exercer les droits des personnes concernées par l'intermédiaire du menu de la plateforme.

[45] Voir les lignes directrices sur la transparence, exemple au point 11.

[46] Pour de plus amples informations sur l'approche à plusieurs niveaux dans un environnement numérique, voir les lignes directrices sur la transparence, points 35 à 37.

Example 17: sur sa plateforme, le fournisseur de médias sociaux met à disposition un document intitulé «*conseils utiles*», qui contient également des informations importantes sur l'exercice des droits des personnes concernées. Toutefois, la politique de confidentialité ne contient aucun lien ni aucune autre indication permettant d'accéder à ce document. Au lieu de cela, elle indique que de plus amples informations sont disponibles dans la section des questions et réponses du site internet. L'utilisateur qui s'attend à trouver des informations sur ses droits dans la politique de confidentialité n'y trouvera donc pas ces explications et devra poursuivre sa navigation et explorer la section des questions et réponses.

82. Cet exemple illustre clairement une interface trompeuse de type ***labyrinthe*** qui rend l'accès à de plus amples informations sur les droits des personnes concernées, et en particulier sur la manière de les exercer, plus difficile qu'il ne devrait l'être, en violation de l'article 12, paragraphe 2, du RGPD. En outre, si la politique de confidentialité est incomplète, cela constitue également une violation de l'article 13, paragraphe 2, points b), c) et d), et de l'article 14, paragraphe 2, points c), d) et e), du RGPD. En effet, alors que les informations plus détaillées ou le moyen direct d'exercer les droits pourraient être accessibles en un seul clic à partir de l'endroit où ils sont mentionnés dans la politique de confidentialité, dans l'exemple, l'utilisateur devra se rendre à la section des questions et réponses et y effectuer une recherche pour trouver le document «*conseils utiles*».

83. Il convient de noter que des effets encore plus importants que ceux causés par un trop grand nombre de niveaux[47] peuvent se produire lorsque l'on utilise non seulement plusieurs appareils, mais aussi plusieurs applications fournies par la même plateforme de médias sociaux, telles que des applications de messagerie spéciales. L'utilisateur qui utilise ce type d'application secondaire serait confronté à des obstacles plus importants et devrait déployer davantage d'efforts s'il devait consulter la version du navigateur ou l'application principale pour obtenir des informations relatives à la protection des données. Dans une telle situation, qui implique non seulement plusieurs appareils mais aussi plusieurs applications, les informations utiles doivent toujours être directement accessibles, quelle que soit la manière dont l'utilisateur utilise la plateforme.

Obstruction – Impasse (annexe I, liste de contrôle 4.4.1)

84. Il peut également y avoir violation des exigences légales lorsque des actions supplémentaires, telles qu'un clic sur un lien ou un bouton, sont nécessaires pour avoir accès aux informations relatives à la protection des données requises par le RGPD. En particulier, une navigation mal orientée ou une conception incohérente de l'interface conduisant à des fonctionnalités inopérantes ne sauraient être considérées comme loyales au sens de l'article 5, paragraphe 1, point a), du RGPD, dès lors que l'utilisateur est induit en erreur lorsqu'il tente soit d'obtenir certaines informations, soit de définir ses préférences en matière de protection des données. Il convient donc, dans tous les cas, d'éviter les ***impasses*** dans lesquelles l'utilisateur se retrouve seul, sans fonctions pour faire valoir ses droits, et qui constituent une violation directe de l'article 12, paragraphe 2, du RGPD, qui indique que le responsable du traitement doit faciliter l'exercice des droits.

Example 18: dans sa politique de confidentialité, un fournisseur de médias sociaux propose de nombreux liens hypertextes vers des pages contenant de plus amples informations sur des thèmes spécifiques. Toutefois, plusieurs parties de la politique de confidentialité ne

[47] Voir points 81 et 82 ci-dessus.

contiennent que des déclarations générales indiquant qu'il est possible d'accéder à de plus amples informations, mais sans préciser où ni comment.

85. La politique de confidentialité est généralement considérée comme le document dans lequel sont centralisées toutes les informations relatives à la protection des données, conformément aux obligations prévues aux articles 12, 13 et 14 du RGPD. Il est dès lors nécessaire de veiller également à ce que l'utilisateur soit redirigé vers toutes les sections pertinentes de la plateforme de médias sociaux où il pourra contrôler ses données ou exercer ses droits. Dans l'exemple 18 ci-dessus, cette mesure n'est que partiellement mise en œuvre, puisque des liens vers de plus amples informations sont fournis pour certains éléments, mais pas pour d'autres. À cet égard, l'interface trompeuse de type ***impasse*** peut donner lieu à une violation de l'article 12, paragraphe 1, du RGPD, en rendant difficile l'accès à certaines informations relatives à la protection des données, ou à une violation de l'article 12, paragraphe 2, du RGPD, en ne facilitant pas l'exercice des droits.

d. **Bonnes pratiques**

Navigation «collée»: lors de la consultation d'une page relative à la protection des données, la table des matières peut rester affichée en permanence sur l'écran, permettant ainsi à l'utilisateur de toujours se situer sur la page et de naviguer rapidement dans le contenu grâce à des liens d'ancrage.

Retour au début de la page: insérer un bouton de retour au début de la page en bas de la page ou un élément fixe au bas de la fenêtre afin de faciliter la navigation de l'utilisateur sur une page.

Raccourcis: pour la définition, voir le cas d'utilisation n° 1 (p. 22) (*par exemple, dans la politique de confidentialité, prévoir, pour chaque information sur la protection des données, des liens qui redirigent directement vers les pages relatives à la protection des données sur la plateforme de médias sociaux*).

Coordonnées: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Contacter l'autorité de contrôle: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Aperçu de la politique de confidentialité: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Détection des changements et comparaison: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Formulation cohérente: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Fournir des définitions: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Utilisation d'exemples: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Cas d'utilisation n° 2b: fournir à la personne concernée des informations sur la responsabilité conjointe du traitement (article 26, paragraphe 2, du RGPD)

a. Description du contexte et des dispositions juridiques pertinentes

86. La deuxième phrase de l'article 26, paragraphe 2, du RGPD prévoit des dispositions supplémentaires en matière de transparence dans le cas spécifique de la responsabilité conjointe du traitement[48].

[48] Pour la définition de la responsabilité conjointe du traitement, voir l'article 4, point 7, lu en combinaison avec l'article 26, paragraphe 1, première phrase, du RGPD, ainsi que les lignes directrices 07/2020 de l'EDPB concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, adoptées le 7 juillet 2021, version 2.1, points 46 à 49, disponibles à l'adresse suivante: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

Celles-ci garantissent que les grandes lignes de l'accord de responsabilité conjointe sont mises à la disposition des personnes concernées[49]. Dans ses lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, l'EDPB recommande que les grandes lignes couvrent à tout le moins l'ensemble des éléments des informations visées aux articles 13 et 14 du RGPD, qui devraient déjà être accessibles à la personne concernée et, pour chaque élément, l'accord devrait préciser quel responsable conjoint du traitement est chargé d'en garantir le respect[50]. Les grandes lignes de l'accord doivent également indiquer le point de contact, s'il a été désigné. Il appartient aux responsables conjoints du traitement de décider du moyen le plus efficace de mettre les grandes lignes de l'accord à la disposition des personnes concernées[51].

b. Interfaces trompeuses

Example 19: en ce qui concerne les interfaces trompeuses, la difficulté pour les responsables du traitement dans ce contexte est d'intégrer ces informations dans le système en ligne de manière à ce qu'elles puissent être perçues aisément et qu'elles restent claires et compréhensibles, bien que la première phrase de l'article 12, paragraphe 1, du RGPD ne fasse pas directement référence à l'article 26, paragraphe 2, deuxième phrase, du RGPD. Toutefois, compte tenu des principes de loyauté, de transparence et de responsabilité en matière de protection des données énoncés à l'article 5, paragraphe 1, point a), et à l'article 5, paragraphe 2, du RGPD, des exigences comparables s'appliquent également en cas de responsabilité conjointe du traitement. Lorsque les responsables conjoints du traitement fournissent des informations sur les grandes lignes de l'accord dans une déclaration de confidentialité, ils doivent aussi le faire de façon claire et transparente. Dès lors, le traitement ne peut plus être considéré comme loyal si les informations le concernant sont difficiles à obtenir en raison de l'absence de liens ou parce que les informations sont disséminées dans plusieurs domaines d'information. L'interface trompeuse de type ***labyrinthe***[52] pourrait être encore plus source de confusion que, d'une manière générale, dans une déclaration de confidentialité, car l'utilisateur peut s'attendre à ce que les informations visées à l'article 26, paragraphe 2, deuxième phrase, du RGPD soient fournies en une seule fois. Dans la politique de confidentialité, un fournisseur de médias sociaux mentionne toujours des «*données de création*» et n'utilise pas l'expression «données à caractère personnel». Ce n'est qu'à la page 90 de la déclaration de confidentialité à plusieurs niveaux qu'il explique que «*les données de création peuvent comprendre des données à caractère personnel des utilisateurs*». Les grandes lignes de l'accord de responsabilité conjointe du traitement fournies aux personnes concernées contiennent également l'expression «données de création», sans explication. L'autre responsable conjoint du traitement (B) donne une définition des données à caractère personnel dans sa propre politique de confidentialité. Cependant, dans la section de sa politique de confidentialité relative à la responsabilité conjointe du traitement avec le fournisseur de médias sociaux, B propose seulement un lien vers l'accord fourni par le fournisseur de médias sociaux, sans autre explication.

[49] Voir les lignes directrices 07/2020 de l'EDPB concernant les notions de responsable du traitement et de sous-traitant, point 179.
[50] Voir les lignes directrices 07/2020 de l'EDPB concernant les notions de responsable du traitement et de sous-traitant, point 180, également pour la phrase suivante.
[51] Lignes directrices 07/2020 de l'EDPB concernant les notions de responsable du traitement et de sous-traitant, point 181.
[52] Voir ci-dessus, cas d'utilisation 2a, exemple 17, des présentes lignes directrices.

87. Les explications prévues à l'article 26, paragraphe 2, deuxième phrase, du RGPD sont plus difficiles à comprendre lorsqu'elles ne sont plus cohérentes. Cet effet d'incohérence est amplifié lorsque les plateformes de médias sociaux utilisent une terminologie propre que l'utilisateur n'associe généralement pas au traitement de données à caractère personnel, comme l'illustre l'exemple 19 ci-dessus. Dans l'exemple, les deux responsables conjoints du traitement violent l'article 26, paragraphe 2, deuxième phrase, du RGPD, ainsi que l'article 5, paragraphe 1, point a), du RGPD, car les informations fournies concernant la responsabilité conjointe du traitement ne sont pas claires et, partant, ne sont pas transparentes pour les personnes concernées.

Cas d'utilisation 2c: communication à la personne concernée d'une violation de données à caractère personnel

a. Description du contexte et des dispositions juridiques pertinentes

88. Pour pouvoir détecter et remédier à une violation de données, le responsable du traitement doit être capable de reconnaître une telle violation[53]. Selon l'article 4, point 12, du RGPD, on entend par «violation de données à caractère personnel» une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données. En ce qui concerne les responsables du traitement des médias sociaux, les violations de données peuvent prendre différentes formes, par exemple lorsque l'auteur d'une attaque réussit à accéder aux données à caractère personnel et aux messages de discussion des utilisateurs. Il est également possible qu'une application, en raison d'une erreur de programmation, accède à des données à caractère personnel auxquelles l'utilisateur n'a pas autorisé l'accès. Un autre exemple serait le cas où l'utilisateur partage des images en sélectionnant l'option «partager avec mes meilleurs amis», pour ensuite constater que ses photos sont mises à la disposition d'un plus grand nombre de personnes. Un dernier exemple serait un bug à cause duquel une plateforme de médias sociaux proposant des vidéos en temps réel continuerait de partager la diffusion en continu de contenus, alors que l'utilisateur a préalablement appuyé sur un bouton pour arrêter l'enregistrement.

89. En cas de violation de données à caractère personnel, le responsable du traitement, en tout état de cause, informe l'autorité de contrôle compétente conformément à l'article 33 du RGPD, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Si une violation de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement, en général, communique également cette violation aux personnes concernées conformément à l'article 34, paragraphes 1 et 2 du RGPD. Dans ce cas, le responsable du traitement doit informer les personnes concernées dans les meilleurs délais. Ces informations doivent décrire en des termes clairs et simples la nature de la violation de données à caractère personnel, étant donné que l'article 12 du RGPD s'applique également. En outre, ces informations doivent contenir à tout le moins des informations et des mesures telles que les suivantes [voir également l'article 33, paragraphe 3, points b) à d), du RGPD, lu en combinaison avec l'article 34, paragraphe 2, du RGPD]:

[53] Voir également les lignes directrices 01/2021 de l'EDPB intitulées «Exemples concernant la notification de violations de données à caractère personnel», adoptées le 14 décembre 2021, version 2.0, point 4, disponibles à l'adresse suivante: https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_fr.pdf

- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;
- une description des conséquences probables de la violation de données à caractère personnel; et
- une description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives[54].

90. Ces communications relatives à des violations de données au titre de l'article 34 du RGPD peuvent également contenir des interfaces trompeuses, par exemple si le responsable du traitement concerné communique à la personne concernée toutes les informations nécessaires pour l'informer de l'ampleur de la violation des données, mais lui communique également des informations non spécifiques et inutiles, ainsi que les conséquences et les mesures de précaution qu'il a prises ou suggère de prendre. Ces informations en partie inutiles peuvent être trompeuses, et l'utilisateur concerné par la violation risque de ne pas comprendre pleinement les conséquences de la violation ou d'en sous-estimer les effets (potentiels).

b. Interfaces trompeuses

91. Pour donner quelques exemples négatifs, les cas présentés ci-dessous peuvent constituer des pratiques abusives en matière de notification de violations de données, contraires à l'article 34 du RGPD, lu en combinaison avec l'article 12 du RGPD.

i. Interfaces trompeuses fondées sur le contenu

Brouillage – Informations contradictoires (annexe I, liste de contrôle 4.6.2)

Example 20:

- le responsable du traitement mentionne uniquement des actions d'un tiers, indiquant que la violation de données a été commise par un tiers (par exemple, un sous-traitant) et que, par conséquent, il n'y a pas eu de violation de la sécurité. Le responsable du traitement met également en évidence certaines bonnes pratiques qui n'ont rien à voir avec la violation elle-même.

- le responsable du traitement déclare la gravité de la violation de données au regard de lui-même ou d'un sous-traitant, plutôt qu'au regard de la personne concernée.

Brouillage – Formulations ou informations ambigües (annexe I, liste de contrôle 4.6.3)

92. En ce qui concerne le langage utilisé pour communiquer la violation à la personne concernée, il est essentiel que les responsables du traitement gardent à l'esprit que la plupart des destinataires ne sont pas habitués au jargon spécifique, voire technique ou juridique, de la protection des données.

Example 21: en raison d'une violation de données sur une plateforme de médias sociaux, plusieurs séries de données de santé ont été accidentellement rendues accessibles à des

[54] Lignes directrices du groupe de travail «Article 29» sur la notification des violations de données à caractère personnel, approuvées par l'EDPB, p. 20, disponibles à l'adresse suivante: https://ec.europa.eu/newsroom/article29/items/612052/en

utilisateurs non autorisés. Le fournisseur de médias sociaux informe uniquement les utilisateurs que des «*catégories particulières de données à caractère personnel*» ont été accidentellement rendues publiques.

93. Il s'agit là d'une ***Formulation ambiguë***, puisque l'utilisateur moyen ne comprend pas l'expression «*catégories particulières de données à caractère personnel*» et ne sait donc pas que ses données de santé ont été divulguées. En effet, le terme «particulières» a une signification très différente dans le langage général de celle qu'il a dans le langage étroit lié au RGPD. L'utilisateur moyen ne sait pas que, au sens de l'article 9 du RGPD, les «*catégories particulières de données à caractère personnel*» signifient les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ou les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. Par conséquent, dans ce scénario, l'appellation «*catégories particulières de données à caractère personnel*» constitue une interface trompeuse, car elle induit l'utilisateur en erreur parce qu'elle n'est accompagnée d'aucune explication. Il s'agit d'un exemple de situation dans laquelle un responsable du traitement tente d'informer les personnes concernées de la violation, mais ne respecte pas pleinement son obligation de communiquer la violation des données conformément à l'article 34 du RGPD, car la gravité de l'incident sera sous-estimée par le lecteur moyen. Les informations succinctes fournies dans l'exemple ne sont pas non plus compréhensibles, comme l'exige l'article 34 du RGPD, lu en combinaison avec l'article 12, paragraphe 1, première phrase, du RGPD.

94. Un autre exemple de ***Formulation ambigüe*** est le suivant:

Example 22: le responsable du traitement ne fournit que de vagues informations lorsqu'il indique les catégories de données à caractère personnel concernées. Par exemple, il fait référence à des documents soumis par les utilisateurs, sans préciser quelles catégories de données à caractère personnel ces documents contiennent et dans quelle mesure ils étaient sensibles.

95. Il importe de faire remarquer que cette interface trompeuse peut survenir dans toutes les parties de la notification de violation de données. Alors que les deux exemples susmentionnés illustrent une formulation peu claire des catégories de données concernées, l'exemple suivant montre que la catégorie des personnes concernées peut être tout aussi peu claire:

Example 23: lorsqu'il signale la violation, le responsable du traitement n'indique pas avec suffisamment de précision la catégorie des personnes concernées. Par exemple, il mentionne uniquement que les personnes concernées étaient des étudiants, mais sans préciser si les personnes concernées sont des mineurs ou des groupes de personnes concernées vulnérables.

96. Enfin, la gravité de l'incident peut également être sous-estimée lorsque des ***informations ambiguës*** sont fournies, comme dans l'exemple ci-dessous:

Example 24: lors de la notification de la violation à l'autorité de contrôle et à la personne concernée, le responsable du traitement déclare que des données à caractère personnel ont été rendues publiques par d'autres sources. La personne concernée considère donc qu'il n'y a pas eu de violation de la sécurité.

ii. Interfaces trompeuses fondées sur le processus de navigation

97. Des exemples négatifs de notifications de violation de données, contraires à l'article 34 du RGPD, lu en combinaison avec l'article 12, du RGPD peuvent également constituer des interfaces trompeuses fondées sur le processus de navigation, comme le montre ce qui suit:

Inattention – Détournement d'attention (annexe I, liste de contrôle 4.2.2)

Example 25:

- le texte du rapport du responsable du traitement sur la violation contient de nombreuses informations inutiles et omet les informations utiles.
- lors de violations de la sécurité concernant des identifiants d'accès et d'autres types de données, le responsable du traitement déclare que les données sont cryptées ou hachées, alors que ce n'est le cas que pour les mots de passe.

98. Dans ce cas, même si les informations utiles figurent dans le rapport, les personnes concernées risquent d'en être détournées par une surcharge d'informations inutiles.

c. Bonnes pratiques

Notifications: les notifications peuvent être utilisées pour sensibiliser l'utilisateur aux aspects, aux changements ou aux risques liés au traitement des données à caractère personnel (*par exemple, en cas de violation de données*). Ces notifications peuvent être mises en œuvre de plusieurs manières, par exemple par des messages dans la boîte de messagerie, des fenêtres «pop-in», des bandeaux fixes en haut de la page internet, etc.

Expliquer les conséquences: lorsque l'utilisateur souhaite activer ou désactiver un outil de contrôle de la protection des données, ou donner ou retirer son consentement, l'informer de manière neutre des conséquences d'une telle action.

Raccourcis: pour la définition, voir le cas d'utilisation n° 1 (p. 22) (*par exemple, fournir à l'utilisateur un lien permettant de réinitialiser son mot de passe*).

Formulation cohérente: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Fournir des définitions: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Utilisation d'exemples: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

3.3 Se protéger sur les réseaux sociaux

Cas d'utilisation n° 3a: gérer son consentement lors de l'utilisation d'une plateforme de médias sociaux

a. Description du contexte et des dispositions juridiques pertinentes

99. Les utilisateurs des plateformes de médias sociaux doivent donner leur consentement à différents stades des activités de traitement des données, par exemple avant de recevoir de la publicité personnalisée. Comme l'EDPB l'a déjà souligné dans ses lignes directrices sur le ciblage des utilisateurs de médias sociaux, le consentement ne peut constituer une base juridique appropriée que si la personne concernée se voit offrir un contrôle et un véritable choix55. En outre, selon l'article 4,

[55] Lignes directrices 08/2020 sur le ciblage des utilisateurs de médias sociaux, point 51.

point 11, du RGPD, le consentement doit être spécifique, éclairé et univoque56. Il importe de souligner que les exigences relatives à la validité du consentement prévues par le RGPD ne constituent pas des obligations supplémentaires mais des conditions préalables à la licéité du traitement des données à caractère personnel des utilisateurs. Par ailleurs, en ce qui concerne les méthodes de commercialisation ou de suivi en ligne, la directive 2002/58/CE (directive «vie privée et communications électroniques») s'applique. Toutefois, les conditions préalables à la validité du consentement figurant dans la directive «vie privée et communications électroniques» sont identiques aux dispositions relatives au consentement énoncées dans le RGPD57.

100. Compte tenu du principe de responsabilité énoncé à l'article 5, paragraphe 2, du RGPD, ainsi que de la nécessité pour le responsable du traitement d'être en mesure de démontrer que la personne concernée a consenti au traitement de ses données à caractère personnel, prévue à l'article 7, paragraphe 1, du RGPD, il est essentiel que le fournisseur de médias sociaux puisse prouver qu'il a dûment obtenu le consentement de l'utilisateur. Cette condition peut s'avérer difficile à prouver, par exemple si l'utilisateur est censé donner son consentement en acceptant les cookies. En outre, la personne concernée ne sait pas toujours qu'elle donne son consentement lorsqu'elle clique rapidement sur un bouton mis en évidence ou sur des options prédéfinies. Néanmoins, comme le souligne l'article 7, paragraphe 1, du RGPD, c'est au responsable du traitement qu'il incombe de prouver que l'utilisateur a librement donné son consentement.

b. Interfaces trompeuses

i. Interfaces trompeuses fondées sur le contenu

101. Outre les interfaces trompeuses fondées sur le contenu expliquées précédemment qui pourraient s'appliquer aux informations relatives à une demande de consentement[58], il existe deux autres interfaces trompeuses fondées sur le contenu en ce qui concerne le consentement.

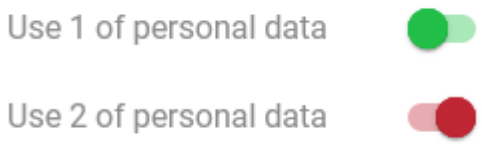
Informations contradictoires – Brouillage (annexe I, liste de contrôle 4.6.2)

Example 26: l'interface utilise un interrupteur pour permettre à l'utilisateur de donner ou de retirer son consentement. Toutefois, la manière dont cet interrupteur est conçu ne permet pas de distinguer clairement la position dans laquelle il se trouve ni de déterminer si l'utilisateur a donné ou non son consentement. En effet, la position de l'interrupteur ne correspond pas à la couleur affichée. Si le bouton se trouve du côté droit, ce qui est généralement associé à l'activation de la fonction («allumer»), la couleur de l'interrupteur est rouge, ce qui signifie généralement qu'une fonction est désactivée. À l'inverse, lorsque le bouton se trouve du côté gauche, ce qui signifie généralement que la fonction est désactivée, la couleur de fond de l'interrupteur est verte, ce qui est normalement associé à une option active.

[56] Voir également les points 25 à 29 ci-dessus.

[57] Voir l'article 2, point f), de la directive 2002/58/CE ainsi que l'avis 5/2019 de l'EDPB relatif aux interactions entre la directive «vie privée et communications électroniques» et le RGPD, en particulier en ce qui concerne la compétence, les missions et les pouvoirs des autorités de protection des données, adopté le 12 mars 2019, point 14, disponible à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_fr

[58] Voir le cas d'utilisation n° 1, points 32 à 49, ou les exemples du cas d'utilisation n° 1 énumérés dans l'annexe.



102. Le fait de fournir des ***informations contradictoires*** lors de la demande de consentement rend ces informations peu claires et difficilement compréhensibles. L'exemple ci-dessus illustre un cas dans lequel les informations visuelles sont équivoques. En effet, face à ces interrupteurs, l'utilisateur ne saura pas avec certitude s'il a donné ou non son consentement. Lorsque les signifiants visuels sont ainsi mélangés ou présentés dans d'autres couleurs qui semblent contradictoires par rapport au contexte (l'exemple 26 ne contenant qu'une seule illustration d'interrupteurs prêtant à confusion), le consentement ne saurait être considéré comme ayant été donné de manière univoque, conformément à l'article 7, paragraphe 2, du RGPD, lu en combinaison avec l'article 4, point 11, du RGPD. Des ***informations contradictoires*** peuvent également être fournies par des moyens textuels, comme indiqué ci-dessous.

Example 27: le fournisseur de médias sociaux communique des informations contradictoires à l'utilisateur: bien que ces informations indiquent dans un premier temps que les contacts ne sont pas importés sans consentement, une fenêtre d'information contextuelle explique en même temps comment les contacts seront importés de toute façon.

Obstruction – Action trompeuse (annexe I, liste de contrôle 4.4.3)

103. Outre des ***informations contradictoires***, les responsables du traitement peuvent fournir des informations qui induisent l'utilisateur en erreur en ne répondant pas à ses attentes. On parle d'***action trompeuse*** lorsqu'un décalage entre les informations et les actions mises à la disposition de l'utilisateur l'incite à faire quelque chose qu'il n'a pas l'intention de faire. Il est probable que la différence entre les attentes de l'utilisateur et le résultat obtenu le dissuade d'aller plus loin.

Example 28: l'utilisateur parcourt son fil d'actualité sur les médias sociaux. Des publicités lui sont présentées durant ce parcours. Intrigué par une annonce et curieux de connaître les raisons pour lesquelles celle-ci lui est présentée, il clique sur un signe «?» affiché dans le coin inférieur droit de la publicité. S'ouvre alors une fenêtre contextuelle qui explique à l'utilisateur pourquoi il voit cette publicité en particulier et énumère les critères de ciblage. Elle les informe également qu'ils peuvent retirer leur consentement à la publicité ciblée et affiche un lien à cet effet. Lorsque l'utilisateur clique sur ce lien, il est redirigé vers un site internet totalement différent donnant des explications générales sur ce qu'est le consentement et sur la manière de le gérer.

104. Le cas ci-dessus est un exemple de contenu qui ne répond pas aux attentes de l'utilisateur. En effet, lorsque l'utilisateur clique sur le lien, il s'attend à être redirigé vers une page qui lui permettra de retirer directement son consentement. Or, la page qui s'affiche ne lui permet pas de le faire et n'indique pas la manière spécifique de retirer son consentement sur la plateforme de médias sociaux. Cette différence entre ce que l'utilisateur est censé trouver et ce qu'il trouve effectivement risque de

le déconcerter et de le laisser dans l'incertitude quant à la marche à suivre. Dans le pire des cas, il pourrait croire qu'il ne peut pas retirer son consentement. Une telle ***action trompeuse*** ne saurait être considérée comme transparente, comme l'exige l'article 12, paragraphe 1, du RGPD. En outre, si l'on compare les modalités de retrait à la manière dont le consentement est obtenu, cette pratique pourrait constituer une violation de l'article 7, paragraphe 3, du RGPD s'il s'avère plus difficile de retirer son consentement que de le donner.

105. Lorsque le fournisseur de médias sociaux informe l'utilisateur qu'une action de sa part peut avoir une certaine conséquence et que l'action aboutit en fait à un résultat différent, il s'agit d'une ***action trompeuse***, comme le montre l'exemple suivant.

> **Example 29:** dans la partie du compte sur les médias sociaux où l'utilisateur peut partager ses réflexions, ses photos, etc., il est invité à confirmer qu'il souhaite partager ce contenu après l'avoir tapé ou téléchargé. L'utilisateur peut choisir de cliquer sur le bouton «*Oui*» ou sur le bouton *«Non».* Toutefois, alors qu'il a décidé de ne pas partager le contenu avec des tiers en cliquant sur le deuxième bouton, le contenu est quand même publié sur son compte.

106. Comme dans l'exemple précédent, ces informations ne sont pas transparentes et privent l'utilisateur de son choix. Même si l'utilisateur remarque rapidement la publication et la supprime à nouveau, les données ont été traitées malgré son refus et mises à la disposition de tiers. La situation est pire encore lorsque, par exemple, l'utilisateur n'a aucun moyen de s'apercevoir du traitement, ou peut s'en apercevoir seulement avec des difficultés ou s'il dispose d'une certaine connaissance des technologies de l'information, parce qu'il a lieu en arrière-plan de la plateforme de médias sociaux.

ii. Interfaces trompeuses fondées sur le processus de navigation

107. Outre les deux interfaces trompeuses ci-dessus, ce sont surtout les interfaces fondées sur le processus de navigation qui sont pertinentes dans ce cas d'utilisation.

Inattention – Détournement d'attention (annexe I, liste de contrôle 4.2.2)

108. Lorsqu'une action ou une information relative à la protection des données est mise en concurrence avec un autre élément lié ou non à la protection des données, et que l'utilisateur choisit cette autre option, il risque d'oublier la première, même s'il s'agissait de son choix initial. L'utilisateur est en présence d'une interface trompeuse de ***détournement d'attention***, qui doit être analysée au cas par cas.

> **Example 30:** un bandeau relatif aux cookies s'affiche sur la plateforme de médias sociaux, indiquant «Pour obtenir de délicieux cookies, vous n'avez besoin que de beurre, de sucre et de farine. Pour voir notre recette préférée, cliquez ici [lien]. Nous aussi, nous utilisons des cookies. Pour en savoir plus, voir notre politique en matière de cookies [lien]», et est accompagné d'un bouton «OK».

109. L'humour ne devrait pas être utilisé pour donner une image erronée des risques potentiels et invalider les informations réelles. Dans cet exemple, l'utilisateur peut être tenté de ne cliquer que sur le premier lien, pour lire la recette des cookies, puis de cliquer sur le bouton «*OK*». Cet exemple illustre un cas dans lequel, outre le fait que l'utilisateur n'a pas la possibilité de ne pas donner son consentement, ce dernier pourrait ne pas être éclairé. En effet, en cliquant sur le bouton «OK», l'utilisateur pourrait

penser qu'il vient de rejeter un message amusant sur des gâteaux appelés «cookies» et ne pas envisager le sens technique du terme «*cookies*». Dans ce cas, son consentement ne constituerait pas un consentement éclairé au sens de l'article 7, paragraphe 2, du RGPD, lu en combinaison avec l'article 4, point 11, du RGPD.

110. L'article 7, paragraphe 2, du RGPD dispose en outre qu'une demande de consentement doit être présentée sous une forme qui la distingue des autres questions. Il est donc nécessaire que les informations relatives à la protection des données ne soient pas éclipsées par d'autres contextes. Dans cet exemple, le jeu de mots avec les homonymes «cookies» peut avoir pour effet que le contexte de la pâtisserie éclipse celui de la protection des données. Afin qu'elles puissent être distinguées aisément, les informations utiles permettant à l'utilisateur de donner un consentement valable devraient être fournies de façon claire, pas «***cachées au grand jour***», et ne pas être mélangées à d'autres questions ou significations. Il ne devrait pas y avoir de confusion possible entre les informations relatives à la protection des données et d'autres types de contenus. Dans le cas contraire, l'attention de l'utilisateur pourrait être détournée des conséquences réelles du traitement de ses données à caractère personnel. Lors de la mise en œuvre de ces conditions préalables, les concepteurs doivent disposer d'une certaine marge de manœuvre pour rendre l'information attractive.

Obstruction – Impasse (annexe I, liste de contrôle 4.4.1)

111. La confusion ou le détournement d'attention n'est pas le seul effet possible des interfaces trompeuses en ce qui concerne le consentement. L'interface trompeuse de type ***impasse,*** en particulier, peut interférer de plusieurs manières avec les conditions de consentement énoncées à l'article 7 du RGPD, lu en combinaison avec l'article 4, point 11, du RGPD.

Example 31: l'utilisateur souhaite gérer les autorisations données à la plateforme de médias sociaux sur la base de son consentement. Il doit trouver une page dans les paramètres qui concerne ces actions spécifiques et souhaite désactiver le partage de ses données à caractère personnel à des fins de recherche. Lorsque l'utilisateur clique sur la case pour la décocher, rien ne se produit au niveau de l'interface et il a l'impression qu'il ne peut pas retirer son consentement.

112. Dans cet exemple spécifique, l'interface trompeuse de type ***impasse*** pourrait violer l'article 7, paragraphe 3, du RGPD, car l'utilisateur n'a apparemment pas la possibilité de retirer son consentement au traitement de ses données à caractère personnel à des fins de recherche, la fonction prévue à cette fin ne fonctionnant manifestement pas. Si l'action de l'utilisateur n'est pas correctement enregistrée dans le système, il y a violation de l'article 7, paragraphe 3, du RGPD. Si le choix est effectivement enregistré dans le système, le fait que l'interface ne reflète pas l'action de l'utilisateur pourrait être considéré comme une violation du principe de loyauté énoncé à l'article 5, paragraphe 1, point a), du RGPD. Lorsqu'une interface semble offrir la possibilité de gérer correctement son consentement, en permettant à l'utilisateur de donner son consentement ou de retirer un consentement précédemment donné, mais qu'elle ne produit aucun effet visuel lorsqu'on interagit avec elle, elle induit l'utilisateur en erreur et crée chez lui de la confusion, voire de la frustration. Il convient d'éviter un tel décalage entre l'état du système et les informations transmises par l'interface, car il peut empêcher l'utilisateur de contrôler ses données à caractère personnel.

113. De nombreuses activités de traitement font intervenir plusieurs parties, c'est-à-dire, outre le responsable du traitement ou le sous-traitant avec lequel la personne concernée est en contact direct, un autre responsable du traitement (conjoint) ou un autre sous-traitant.

Example 32: un fournisseur de médias sociaux collabore avec des tiers aux fins du traitement des données à caractère personnel de ses utilisateurs. Dans sa politique de confidentialité, il communique la liste de ces tiers sans proposer de lien vers leur politique de confidentialité, invitant simplement l'utilisateur à consulter les sites internet des tiers afin d'obtenir des informations sur la manière dont ces entités traitent les données et la manière d'exercer ses droits.

114. Cet exemple d'interface trompeuse de type ***impasse*** montre comment l'accès aux informations relatives au traitement est rendu plus difficile pour l'utilisateur. Étant donné qu'il n'obtiendra probablement pas toutes les informations utiles sur le traitement, une telle pratique pourrait être considérée comme une violation des exigences aux informations aisément accessibles énoncées à l'article 12, paragraphe 1, du RGPD. Si cette pratique est appliquée à des informations fournies en vue d'obtenir le consentement de l'utilisateur, elle peut constituer une violation des exigences relatives au consentement éclairé énoncées à l'article 7, paragraphe 2, du RGPD, lu en combinaison avec l'article 4, point 11, du RGPD, puisque les informations seraient trop difficiles à trouver et les personnes concernées n'auraient donc pas pleinement conscience des conséquences de leur choix.

Obstruction – Processus plus long que nécessaire (annexe I, liste de contrôle 4.4.2)

115. L'article 7, paragraphe 3, du RGPD dispose qu'il doit être aussi simple de retirer que de donner son consentement. Les lignes directrices 05/2020 sur le consentement au sens du règlement (UE) nº 2016/679 donnent davantage d'informations à ce sujet, indiquant que le consentement devrait être donné et retiré par le même biais. Cela suppose d'utiliser la même interface, mais également que les mécanismes de retrait du consentement soient aisément accessibles, par exemple au moyen d'un lien ou d'une icône disponible à tout moment lors de l'utilisation de la plateforme de médias sociaux.

Example 33: un fournisseur de médias sociaux ne prévoit pas d'option de refus («opt-out») direct du traitement à des fins de publicité ciblée, alors qu'un seul clic suffit pour donner son consentement («opt-in»).

116. Le temps nécessaire ou le nombre de clics requis pour retirer son consentement peut servir à déterminer si le retrait est effectivement aisé. La mise en œuvre de l'interface trompeuse de type ***processus plus long que nécessaire*** dans le parcours de l'utilisateur pour retirer son consentement, comme le montre l'exemple 33, va à l'encontre de ces principes, violant ainsi l'article 7, paragraphe 3, du RGPD.

Surcharge – Labyrinthe (annexe I, liste de contrôle 4.1.2)

117. Comme l'EDPB l'a souligné dans les lignes directrices 05/2020 sur le consentement, il est indispensable de fournir des informations sur le traitement aux personnes concernées avant d'obtenir leur consentement afin de leur permettre de prendre une décision en toute connaissance de cause[59]. Sans cela, le consentement ne saurait être considéré comme valable. Ces mêmes lignes directrices décrivent plus en détail les différentes manières de fournir les informations, en précisant que les informations peuvent être superposées. Toutefois, comme indiqué dans le cas d'utilisation n° 2a[60], les fournisseurs de médias sociaux doivent veiller à éviter les interfaces trompeuses de type ***labyrinthe*** lorsqu'ils

[59] Lignes directrices 05/2020 sur le consentement, points 62 à 64.
[60] Voir points 79 à 81 ci-dessus.

présentent les informations liées à une demande de consentement sur plusieurs niveaux. Si certaines informations deviennent trop difficiles à trouver parce que la personne concernée doit naviguer parmi plusieurs pages ou documents, le consentement obtenu sur la base de ces informations ne peut pas être considéré comme éclairé, ce qui va à l'encontre de l'article 7 du RGPD, lu en combinaison avec l'article 4, point 11, du RGPD. Par extension, cela signifie que le consentement n'est pas valable et que le fournisseur de médias sociaux agit en violation de l'article 6 du RGPD.

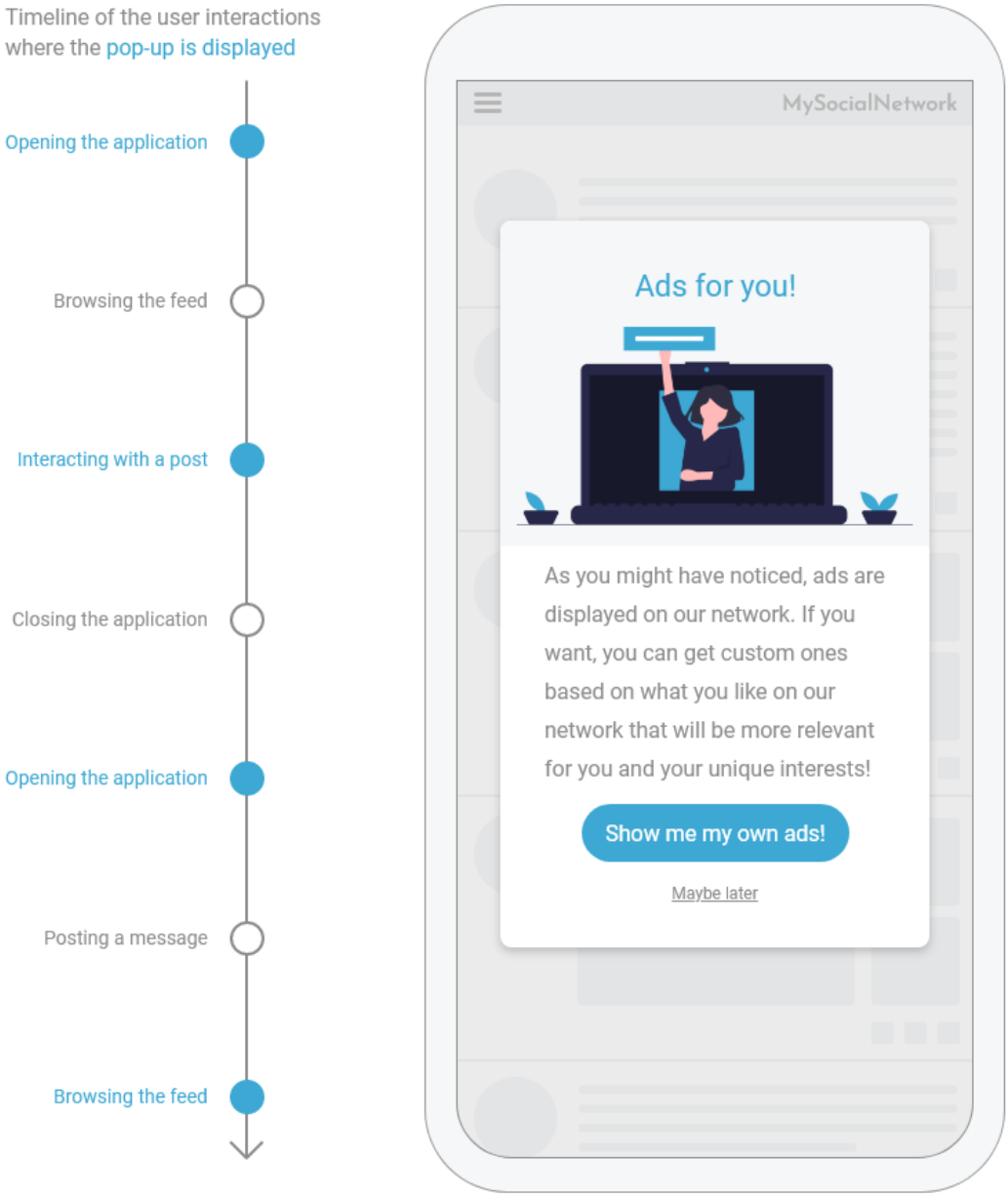
Example 34: les informations relatives au retrait du consentement sont disponibles à partir d'un lien auquel l'utilisateur n'a accès qu'après avoir parcouru chaque section de son compte et les informations associées aux publicités affichées sur son fil d'actualité.

118. Comme le montre le scénario décrit ci-dessus, l'interface trompeuse de type ***Labyrinthe*** peut également poser problème après l'obtention du consentement, du fait du non-respect de la condition prévue à l'article 7, paragraphe 3, quatrième phrase, du RGPD, selon laquelle il est aussi simple de retirer que de donner son consentement. Cela est notamment dû au fait que le processus de retrait du consentement comporte davantage d'étapes que l'action positive consistant à donner son consentement. Étant donné que les informations fournies ne sont pas non plus aisément accessibles pour la personne concernée, puisqu'elles sont réparties sur différentes parties de la page, le principe énoncé à l'article 12, paragraphe 1, du RGPD n'est pas respecté.

Surcharge – Incitation répétitive (annexe I, liste de contrôle 4.1.1)

119. L'***incitation répétitive***, lorsqu'elle est utilisée à l'égard d'utilisateurs qui n'ont pas consenti au traitement de leurs données à caractère personnel pour une finalité spécifique, crée un obstacle à l'utilisation régulière des médias sociaux. Cela signifie que l'utilisateur ne peut pas refuser de donner son consentement ni, par extension, le retirer sans subir de préjudice. Cette pratique va à l'encontre de la condition relative au consentement librement donné prévue à l'article 7 du RGPD, lu en combinaison avec l'article 4, point 11, du RGPD, selon laquelle le consentement est toute manifestation de volonté libre par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement. La cinquième phrase du considérant 42 du RGPD affirme en outre que le consentement ne devrait pas être considéré comme ayant été donné librement si l'utilisateur ne dispose pas d'une véritable liberté de choix. Cela est également confirmé par les lignes directrices de l'EDPB sur le consentement, qui expliquent que le consentement ne sera pas valable si la personne concernée n'est pas véritablement en mesure d'exercer un choix ou se sent contrainte de consentir par tout élément de pression ou d'influence inappropriée sur elle, qui l'empêche d'exercer sa libre volonté[61]. Dès lors que l'***incitation répétitive*** peut engendrer un tel type de pression, elle viole le principe du consentement librement donné. En outre, étant donné qu'il est peu probable qu'une fois que l'utilisateur a donné son consentement, le fournisseur de médias sociaux lui offre régulièrement (par exemple, chaque fois qu'il se connecte à son compte) la possibilité de le retirer, cette interface trompeuse peut violer l'article 7, paragraphe 3, quatrième phrase, du RGPD, qui prévoit qu'il doit être aussi simple de retirer que de donner son consentement («effet miroir»).

[61] Lignes directrices 05/2020 sur le consentement, points 13 et 14.



Example 35: dans cet exemple, lorsque l'utilisateur crée son compte, il lui est demandé s'il accepte que ses données soient traitées afin de recevoir de la publicité personnalisée. S'il ne donne pas son consentement à l'utilisation de ses données lors de son inscription, il voit régulièrement apparaître, lorsqu'il utilise le réseau social, la boîte de dialogue illustrée ci-dessus, qui lui demande s'il souhaite recevoir des publicités personnalisées. Cette boîte l'empêche d'utiliser le réseau social. L'***incitation répétitive*** s'affichant régulièrement, il est probable qu'elle lasse l'utilisateur, qui finira par donner son consentement pour recevoir de la publicité personnalisée. En outre, la pratique ***caché au grand jour***[62] est également utilisée dans cette interface, car l'action d'accepter les publicités est bien plus visible que la possibilité de refuser.

[62] Voir le point 49 ci-dessus ou, ci-dessous, la partie 4.3.2 de l'annexe.

120. De surcroît, le responsable du traitement pourrait violer le principe de loyauté au sens de l'article 5, paragraphe 1, point a), du RGPD. Étant donné que dans l'exemple ci-dessus, l'utilisateur n'a pas consenti, par une action claire, au traitement de ses données à caractère personnel à des fins de publicité ciblée lors de la création de son compte, le fait que l'incitation répétitive remette constamment en question un refus qu'il a clairement exprimé est pénible. Ce choix clair que l'utilisateur a effectué au cours de la procédure d'enregistrement est à présent constamment remis en question. La dégradation de l'expérience utilisateur qui en résulte accroît considérablement la probabilité que l'utilisateur accepte de recevoir de la publicité ciblée à un moment ou à un autre, simplement pour éviter que la question lui soit à nouveau posée chaque fois qu'il se connecte à son compte et qu'il souhaite utiliser la plateforme de médias sociaux. Dans ce cas, le fait de ne pas donner son consentement a une incidence directe sur la qualité du service fourni à l'utilisateur et conditionne l'exécution du contrat.

c. Bonnes pratiques

Cohérence entre les différents appareils: lorsque la plateforme de médias sociaux est accessible à partir de différents appareils (par exemple, ordinateur, smartphones, etc.), les informations et les paramètres relatifs à la protection des données devraient se trouver aux mêmes endroits dans les différentes versions et être accessibles par le même biais et les mêmes éléments d'interface (menu, icônes, etc.).

Détection des changements et comparaison: pour la définition, voir le cas d'utilisation n° 1 (p. 22)**.**

Formulation cohérente: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Fournir des définitions: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Utilisation d'exemples: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Navigation «collée»: pour la définition, voir le cas d'utilisation n° 2a (p. 28).

Retour au début de la page: pour la définition, voir le cas d'utilisation n° 2a (p. 28).

Notifications: pour la définition, voir le cas d'utilisation n° 2c (p. 32).

Expliquer les conséquences: pour la définition, voir le cas d'utilisation n° 2c (p. 32).

Cas d'utilisation n° 3b: gestion de ses paramètres de protection des données

a. Description du contexte

121. À l'issue du processus d'inscription, et pendant toute la durée de vie de son compte sur les médias sociaux, l'utilisateur devrait être en mesure de modifier ses paramètres de protection des données.

122. Qu'il ait ou non une connaissance préalable de la protection des données en général et du RGPD en particulier, et qu'il soit ou non attentif aux données à caractère personnel qu'il souhaite ou ne souhaite pas partager et rendre visibles à des tiers, tout utilisateur a le droit d'être informé de ses possibilités de manière transparente lors de l'utilisation d'un réseau social.

123. Les utilisateurs partagent une grande quantité de données à caractère personnel sur les plateformes de médias sociaux. Ces plateformes les encouragent souvent à continuer de partager régulièrement davantage de données. Si un utilisateur peut souhaiter partager des moments de sa vie, participer à

un débat sur un thème spécifique ou élargir son réseau de contacts, que ce soit pour des raisons professionnelles ou personnelles, il doit également disposer des outils lui permettant de contrôler quel public peut voir quelles parties de ses données à caractère personnel. Un moyen d'éviter de multiplier le nombre d'actions requises pour modifier ses paramètres serait de créer un tableau de bord sur la protection de la vie privée permettant de centraliser les paramètres et de faciliter le contrôle des données des utilisateurs.

b. Dispositions juridiques pertinentes

124. Comme indiqué ci-dessus[63], l'un des grands principes régissant le traitement des données à caractère personnel est établi à l'article 5, paragraphe 1, point a), du RGPD, qui dispose que les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée («licéité, loyauté et transparence»). En vertu du principe de responsabilité énoncé à l'article 5, paragraphe 2, du RGPD, le responsable du traitement est tenu de montrer quelles mesures il prend pour s'assurer que ses activités de traitement sont non seulement licites et loyales, mais aussi transparentes. En outre, le principe de minimisation des données énoncé à l'article 5, paragraphe 1, point c), et le principe de protection des données dès la conception et de protection des données par défaut énoncé à l'article 25 du RGPD sont pertinents aux fins du présent cas d'utilisation.

c. Interfaces trompeuses

i. Interfaces trompeuses fondées sur le contenu

125. La première difficulté rencontrée par l'utilisateur dans ce contexte consiste à savoir où se trouvent les paramètres relatifs à la protection des données. Il pourrait lire l'avis relatif à la protection des données et décider ensuite d'effectuer des changements concernant le traitement de ses données à caractère personnel. Il pourrait également souhaiter procéder à des changements sans avoir lu l'avis, simplement lors de son utilisation habituelle des médias sociaux, par exemple lorsqu'il réalise qu'une information qu'il a publiée sur une plateforme de médias sociaux (par exemple, une photo de famille sur la plage) est partagée avec un groupe de personnes avec lesquelles il ne souhaite pas la partager (par exemple, des collègues). Dans tous les cas, le principe de transparence exige que les options de paramétrage soient aisément accessibles et compréhensibles. La centralisation des paramètres de données et de protection de la vie privée en un seul et même endroit au moyen d'une URL explicite telle que [réseau-social.com]/données-paramètres pourrait permettre d'atteindre cet objectif.

126. Plusieurs interfaces trompeuses liées à cette question rendent la localisation de ces paramètres difficile pour l'utilisateur. Les concepteurs de plateformes de médias sociaux devraient donc veiller à éviter ces interfaces.

Surcharge – Trop nombreuses options (annexe I, liste de contrôle 4.1.3)

127. Les paramètres de protection des données doivent être aisément accessibles et ordonnés de manière logique. Les paramètres relatifs à un même aspect de la protection des données devraient de préférence se trouver en un seul et même endroit bien visible. Dans le cas contraire, l'utilisateur sera contraint de consulter et de parcourir un trop grand nombre de pages, ce qui rendra très laborieux le paramétrage de ses préférences en matière de protection des données. En effet, face à de ***trop nombreuses options***, il peut se trouver dans l'incapacité de faire un choix ou omettre certains

[63] Voir points 1, 9, 10, et 14 à 16, ci-dessus.

paramètres, et finir par abandonner ou passer à côté des paramètres de ses préférences en matière de protection des données. Cette pratique viole les principes de transparence et de loyauté. Elle peut notamment violer l'article 12, paragraphe 1, du RGPD, soit parce qu'elle rend difficile l'accès à un outil spécifique de contrôle de la protection des données car celui-ci est disséminé sur plusieurs pages, soit parce qu'elle rend floue la différence entre les différentes options proposées à l'utilisateur.

Example 36: l'utilisateur risque de ne pas savoir quoi faire face au menu d'une plateforme de médias sociaux contenant plusieurs onglets relatifs à la protection des données: «*protection des données*», «*sécurité*», «*contenu*», «*protection de la vie privée*», «*vos préférences*».

128. Dans cet exemple, l'intitulé des onglets n'indique pas clairement le contenu auquel l'utilisateur peut s'attendre sur la page qui y est associée ou qu'ils sont tous liés à la protection des données, en particulier lorsque l'un des onglets porte spécifiquement ce nom. Cela risque donc d'empêcher l'utilisateur de procéder à des modifications. Par exemple, s'il souhaite limiter ou élargir le nombre de personnes qui peuvent voir les images qu'il a téléchargées, l'intitulé des onglets pourrait l'amener à cliquer sur «sécurité» s'il pense que le fait de rendre ses données accessibles au public peut poser des risques pour la sécurité; sur «contenu», car l'utilisateur souhaite définir les paramètres de visibilité de son post; ou sur «protection de la vie privée», étant donné que cette notion spécifique est directement liée à ce que les personnes souhaitent partager avec des tiers. Cela signifie que ces intitulés ne sont pas suffisamment clairs par rapport à l'action que l'utilisateur souhaite effectuer. En particulier, les expressions «protection des données» et «protection de la vie privée» sont souvent utilisées comme synonymes et prêtent donc particulièrement à confusion si elles sont présentées comme des sections différentes.

Brouillage – Informations contradictoires (annexe I, liste de contrôle 4.6.2)

129. Comme cela a déjà été décrit dans l'exemple 12 et illustré plus en détail dans l'exemple suivant, l'utilisateur peut également recevoir des ***informations contradictoires*** dans le cadre des paramètres de protection des données.

Example 37: l'utilisateur X désactive la fonction de géolocalisation à des fins publicitaires. Après avoir cliqué sur l'interrupteur prévu à cet effet, un message s'affiche, qui indique ce qui suit: «*Nous avons désactivé votre géolocalisation, mais votre localisation sera toujours utilisée*.»

Surcharge – Labyrinthe (annexe I, liste de contrôle 4.1.2)

130. Le principe de loyauté requiert également que, lorsque l'utilisateur modifie un paramètre de protection des données, le fournisseur de médias sociaux l'informe d'autres paramètres similaires. Si ces paramètres sont disséminés sur différentes pages de la plateforme de médias sociaux non reliées entre elles, l'utilisateur risque de passer à côté d'un ou de plusieurs moyens de contrôler un aspect de ses données à caractère personnel. Il s'attend à trouver les paramètres connexes les uns à côté des autres.

Example 38: les thèmes connexes, tels que les paramètres liés au partage de données avec des tiers, et vice versa, par le fournisseur de médias sociaux, ne sont pas proposés aux mêmes endroits ou à des endroits proches, mais sous des onglets différents du menu des paramètres.

131. Il n'existe pas d'approche unique en ce qui concerne le nombre moyen d'actions que l'utilisateur de plateformes de médias sociaux est disposé à exécuter pour modifier un paramètre. Dans le même temps, si elles sont trop nombreuses, l'utilisateur peut être dissuadé d'aller jusqu'au bout de la modification ou passer à côté de certaines parties, en particulier s'il souhaite apporter plusieurs modifications. Entraver de la sorte la volonté des utilisateurs constitue une violation des principes de loyauté énoncés à l'article 5, paragraphe 1, point a), du RGPD. En outre, la modification des paramètres est étroitement liée à l'exercice des droits des personnes concernées[64]. La modification d'un paramètre lié aux données, comme la correction de son nom ou la suppression de l'année d'obtention de son diplôme, peut être considérée comme un exercice du droit de rectification ou du droit d'effacement de ces données spécifiques. Le nombre d'actions requises devrait donc être aussi limité que possible. Bien qu'il puisse varier, un nombre excessif d'actions constitue un obstacle pour l'utilisateur et donc une violation du principe de loyauté, ainsi que de l'article 12, paragraphes 1 et 2, du RGPD.

Inconstance – Discontinuité linguistique (annexe I, liste de contrôle 4.5.4)

132. En ce qui concerne la transparence des informations, les concepteurs de plateformes de médias sociaux doivent également veiller à éviter les interfaces trompeuses fondées sur le contenu énumérées dans le cas d'utilisation 2a, telles que la ***discontinuité linguistique***. Lorsque les pages de paramètres (ou des parties de celles-ci) ne sont pas affichées dans la langue choisie par l'utilisateur pour utiliser la plateforme de médias sociaux, il est plus difficile pour celui-ci de comprendre ce qu'il peut modifier et donc de définir ses préférences.

Inconstance – Interface incohérente (annexe I, liste de contrôle 4.5.3)

133. Dans ce contexte, un autre problème se pose lorsque les plateformes de médias sociaux proposent à l'utilisateur des choix propices à la protection des données, mais sans lui fournir d'informations claires à ce sujet. Tel peut être le cas lorsque la plateforme de médias sociaux diffère soudainement de son interface habituelle. On parle d'***interface incohérente*** lorsqu'une interface manque de cohérence dans différents contextes ou n'est pas cohérente avec les attentes de l'utilisateur. Ces différences peuvent empêcher l'utilisateur de trouver l'outil de contrôle ou l'information souhaité, ou l'amener à interagir avec un élément de l'interface par habitude, même si cette interaction le conduit à faire un choix contre son gré en matière de protection des données.

Example 39: sur l'ensemble de la plateforme de médias sociaux, neuf options sur dix des paramètres de protection des données sont présentées dans l'ordre suivant:

- option la plus restrictive (c'est-à-dire partager le moins de données avec des tiers)
- option limitée, mais pas aussi restrictive que la première
- option la moins restrictive (c'est-à-dire partager le plus de données avec des tiers).

Les utilisateurs de cette plateforme sont habitués à ce que leurs paramètres de protection des données soient présentés dans cet ordre. Or, cet ordre n'est pas appliqué dans le cas du dernier paramètre, pour lequel le choix de la visibilité de la date d'anniversaire de l'utilisateur est indiqué dans l'ordre suivant:

[64] Voir ci-dessous les cas d'utilisation 4 et 5, c'est-à-dire les parties 3.4 et 3.5 des présentes lignes directrices.

- *Montrer ma date d'anniversaire complète*: *15 janvier 1929* (= option la moins restrictive)

- *Montrer uniquement le jour et le mois*: *15 janvier* (= option limitée, mais pas la plus restrictive)

- *Ne pas montrer ma date d'anniversaire à des tiers* (= option la plus restrictive).

134. Dans cet exemple, les trois choix du dernier paramètre sont présentés dans un ordre différent de celui des paramètres précédents. L'utilisateur qui a précédemment modifié ses autres paramètres est probablement habitué à l'ordre «habituel» des neuf premiers paramètres. Pour le dernier paramètre, il est tellement habitué à cet ordre qu'il choisit instinctivement la première option, en supposant qu'il s'agit de la plus restrictive. Le fait d'organiser les options d'un paramètre de protection des données si différemment par rapport aux autres paramètres proposés sur la même plateforme de médias sociaux constitue une ***Interface incohérente***, car cette pratique joue avec les habitudes et les attentes des utilisateurs. Cela peut créer de la confusion chez l'utilisateur ou lui donner l'impression qu'il a fait le choix qu'il souhaitait alors que tel n'est pas le cas en réalité.

ii. Interfaces trompeuses fondées sur le processus de navigation

135. Le deuxième problème rencontré dans le cadre des paramètres de protection des données est que ces paramètres pourraient violer le principe de protection des données par défaut. L'article 25, paragraphe 1, du RGPD impose aux responsables du traitement de prendre des mesures appropriées pour mettre en œuvre les principes relatifs à la protection des données, tels que la minimisation des données [article 5, paragraphe 1, point c), du RGPD]. Ces dispositions ne sont pas respectées lorsque les paramètres de partage des données à caractère personnel sont réglés par défaut sur l'une des options les plus intrusives plutôt que sur la moins intrusive.

Inattention – Confort trompeur (annexe I, liste de contrôle 4.2.1)

Example 40: Parmi les options de visibilité des données «*visible pour moi*», «*pour mes amis les plus proches*» «*pour tous mes contacts*» et «*public*», c'est l'option médiane «*pour tous mes contacts*» qui est définie par défaut. Cela signifie que tous les utilisateurs qui sont connectés à cette personne peuvent voir ses contributions, ainsi que toutes les informations qu'elle a enregistrées lors de son inscription sur la plateforme, telles que son adresse électronique ou sa date de naissance.

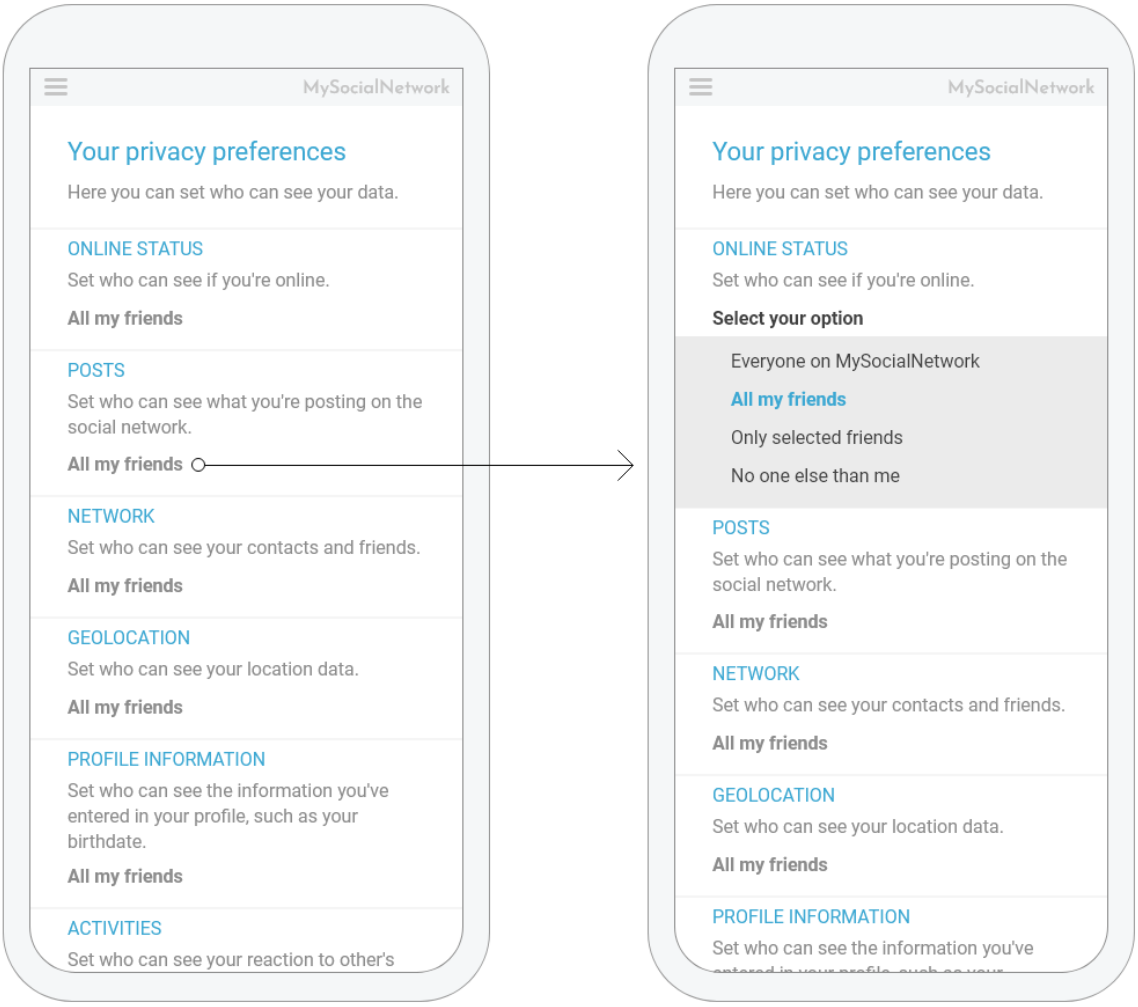
136. Les fournisseurs de médias sociaux pourraient avancer que le paramètre le moins intrusif irait à l'encontre de l'objectif que poursuivent les utilisateurs d'une plateforme de médias sociaux donnée, par exemple le fait d'être contacté par des inconnus pour se faire un nouvel ami, avoir un rendez-vous amoureux ou trouver un emploi. Si cela peut être vrai pour certains paramètres particuliers, les fournisseurs de médias sociaux doivent garder à l'esprit que ce n'est pas parce que l'utilisateur télécharge certaines données sur le réseau qu'il consent à partager ces données avec des tiers[65]. Lorsque les fournisseurs de médias sociaux s'affranchissent de la protection des données par défaut, ils doivent veiller à en informer dûment l'utilisateur. Cela signifie que l'utilisateur doit être informé du ou des paramètres définis par défaut, de l'existence d'options moins intrusives, et de la section de la plateforme où il doit se rendre pour effectuer des changements. Dans l'exemple donné, cela signifie que lorsque l'option «*pour mes amis les plus proches*» est définie par défaut pour les contributions que l'utilisateur poste activement sur la plateforme de médias sociaux, il convient d'indiquer où ce

[65] Par exemple, sa date de naissance; voir point 58 ci-dessus.

paramètre peut être modifié. Toutefois, le fait de définir par défaut la visibilité pour «*tous les contacts de l'utilisateur*» (voire pour le grand public) constitue un ***confort trompeur***, en particulier lorsqu'elle est appliquée aux données que le fournisseur de médias sociaux a exigées de l'utilisateur pour créer un compte, telles que son adresse électronique ou sa date de naissance. Comme décrit dans le cas d'utilisation 1, point 55, cette pratique constitue une violation de l'article 25, paragraphe 2, du RGPD.

Incitation – Caché au grand jour (annexe I, liste de contrôle 4.3.2)

137. Les interfaces trompeuses de type ***caché au grand jour*** et ***confort trompeur*** peuvent facilement être combinées lorsqu'il s'agit de sélectionner des options liées à la protection des données, comme le montre l'exemple 9 pour le processus d'inscription, et comme illustré ci-dessous, lorsque l'utilisateur souhaite modifier ses préférences en matière de protection des données dans le cadre de son utilisation des médias sociaux.



Example 41: dans cet exemple, lorsque l'utilisateur souhaite gérer la visibilité de ses données, il doit aller dans l'onglet «*préférences en matière de protection de la vie privée*». C'est là que sont énumérées les informations pour lesquelles il peut définir ses préférences. Toutefois, la manière dont ces informations sont présentées n'indique pas clairement comment modifier les paramètres. En effet, l'utilisateur doit cliquer sur l'option de visibilité actuellement sélectionnée pour accéder à un menu déroulant à partir duquel il peut sélectionner l'option qu'il préfère.

138. Bien qu'il ait la possibilité de modifier ses préférences sous cet onglet, elle est ***cachée au grand jour*** car le menu déroulant n'est pas directement visible pour l'utilisateur, qui doit deviner qu'un clic sur l'option sélectionnée permettra de l'ouvrir. Il n'existe en effet aucune indication visuelle habituelle (texte souligné, flèche vers le bas) de la possibilité d'interagir et d'ouvrir le menu déroulant. Cette pratique spécifique est déloyale envers les utilisateurs et pourrait contribuer à un non-respect général

du principe de loyauté énoncé à l'article 5, paragraphe 1, point a), du RGPD. En outre, si les options ont été présélectionnées par défaut, on pourrait également être en présence d'une l'interface trompeuse de type ***confort trompeur***, telle que décrite au point 128 ci-dessus.

Inconstance – Décontextualisation (annexe I, liste de contrôle 4.5.2)

139. On parle de ***décontextualisation*** lorsqu'une information ou un outil de contrôle en lien avec la protection des données se trouve sur une page hors contexte, de sorte qu'il est peu probable que l'utilisateur les trouve car il ne les rechercherait pas intuitivement sur cette page spécifique.

> **Example 42:** les paramètres de protection des données sont difficiles à trouver dans le compte utilisateur car, au premier niveau, aucun chapitre du menu ne porte un nom ou un titre qui orienterait dans cette direction. L'utilisateur doit consulter d'autres sous-menus, tels que le sous-menu «*Sécurité*».

140. Dans cet exemple, l'utilisateur n'est pas guidé vers les paramètres de protection des données, car aucun terme explicite et clair n'est utilisé pour indiquer où ces paramètres se trouvent sur la plateforme. En effet, le terme «*Sécurité*» ne couvre qu'une partie de ce que l'on peut attendre des paramètres de protection des données. Il n'est donc pas intuitif pour l'utilisateur de consulter ce menu pour trouver de tels paramètres. Ce manque de transparence rend l'accès à l'information plus difficile qu'il ne devrait l'être et peut être considéré comme contraire à l'article 12, paragraphe 1, du RGPD, et potentiellement à l'article 12, paragraphe 2, du RGPD si ces paramètres concernent l'exercice d'un droit.

> **Example 43:** la modification des paramètres est entravée puisque, dans la version de bureau de la plateforme de médias sociaux, le bouton «*sauvegarder*» permettant d'enregistrer les modifications n'apparaît pas avec toutes les options, mais uniquement en haut du sous-menu. Il est probable que l'utilisateur ne le remarque pas et suppose à tort que ses paramètres sont sauvegardés automatiquement, de sorte qu'il passe à une autre page sans cliquer sur le bouton «*sauvegarder*». Ce problème ne se pose pas dans l'application et la version mobile. Par conséquent, cela ajoute à la confusion de l'utilisateur qui passe de la version mobile/l'application à la version de bureau, et peut l'amener à penser qu'il ne peut modifier ses paramètres que dans la version mobile ou l'application.

141. Dès lors que l'utilisateur a trouvé les paramètres de protection des données et défini ses choix, il ne peut pas être empêché de les modifier. Lorsque l'utilisateur a effectué une modification, la manière de la sauvegarder doit être évidente: soit la sauvegarde intervient dès que l'utilisateur modifie un paramètre, soit l'utilisateur doit confirmer la modification en cliquant sur un élément spécifique de l'interface, par exemple un bouton «sauvegarder». En outre, le principe de loyauté énoncé à l'article 5, paragraphe 1, point a), du RGPD requiert que les fournisseurs de médias sociaux soient cohérents sur l'ensemble de leur plateforme, en particulier sur les différents appareils. Tel n'est pas le cas lorsqu'une interface trompeuse est utilisée comme le décrivent les exemples ci-dessus.

d. Bonnes pratiques

Répertoire de la protection des données: pour permettre à l'utilisateur de naviguer facilement dans les différentes sections du menu, lui présenter une page aisément accessible à partir de laquelle il aura accès à toutes les actions (par exemple, les paramètres) et informations relatives à la protection des données. Cette page peut se trouver dans le menu de navigation principal du fournisseur de médias sociaux, dans le compte d'utilisateur, dans la politique de confidentialité, etc.

Options groupées: combiner des options ayant la même finalité de traitement, afin que l'utilisateur puisse les modifier plus facilement, tout en lui laissant la possibilité de procéder à des changements plus précis. Si les plateformes de médias sociaux présentent des options groupées, celles-ci ne devraient pas contenir d'éléments inattendus ou sans lien entre eux (par exemple, des éléments ayant des finalités différentes). Si le traitement nécessite un consentement, les options groupées doivent être conformes aux lignes directrices de l'EDPB sur le consentement, en particulier à leurs points 42 à 44.

Raccourcis: pour la définition, voir le cas d'utilisation n° 1 (p. 22) (*par exemple, lorsque l'utilisateur est informé d'un aspect du traitement, il est invité à définir ses préférences en matière de données sur la page correspondante des paramètres/du tableau de bord*).

URL explicite: les pages concernant les informations ou les paramètres relatifs à la protection des données doivent avoir une adresse web qui reflète clairement leur contenu. Par exemple, une page centralisant le contrôle de la protection des données pourrait avoir une URL telle que [réseau-social.com]/paramètres-données.

Formulation cohérente: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Fournir des définitions: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Utilisation d'exemples: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Navigation «collée»: pour la définition, voir le cas d'utilisation n° 2a (p. 28).

Notifications: pour la définition, voir le cas d'utilisation n° 2c (p. 32).

Expliquer les conséquences: pour la définition, voir le cas d'utilisation n° 2c (p. 32)**.**

Cohérence entre les différents appareils: pour la définition, voir le cas d'utilisation n° 3a (p. 39).

3.4 Bien se comporter sur les réseaux sociaux: les droits des personnes concernées

Cas d'utilisation n° 4: comment fournir des fonctions appropriées pour l'exercice des droits des personnes concernées

a. Description du contexte

142. Utiliser une plateforme de médias sociaux signifie tirer parti de ses fonctions conformément aux finalités indiquées par le fournisseur de médias sociaux. Cela signifie également que l'utilisateur peut exercer ses droits en matière de protection des données. Ces droits sont des éléments essentiels de la protection des données et du contrôle de ses propres informations, que les données soient fournies directement et sciemment par la personne concernée ou fournies par celle-ci grâce à l'utilisation du service ou du dispositif, ou qu'elles soient déduites de l'analyse des données fournies par la personne concernée[66]. Compte tenu de la quantité de données à caractère personnel circulant sur la plateforme, il est indispensable de permettre à l'utilisateur de contrôler ses données en exerçant les droits prévus par le RGPD de manière claire et intuitive. L'EDPB a expliqué ces notions dans plusieurs documents de

[66] Voir les lignes directrices du groupe de travail «Article 29» relatives au droit à la portabilité des données au titre du règlement (UE) 2016/679, WP242 rev.01, p. 12, https://ec.europa.eu/newsroom/article29/items/611233/en

lignes directrices[67]. L'utilisateur doit pouvoir exercer ces droits dès le début et jusqu'à la fin de l'utilisation de la plateforme et, dans certains cas, même après qu'il a décidé de quitter la plateforme et alors que le responsable du traitement n'a pas encore supprimé ses données. Les non-utilisateurs de la plateforme doivent également pouvoir exercer les droits conférés à la personne concernée à l'égard du traitement de leurs données. Bien entendu, dans certains cas, selon la base juridique du traitement des données, les droits des personnes concernées ne sont pas tous applicables. Le fournisseur de médias sociaux devrait donc également expliquer clairement pourquoi certains droits ne s'appliquent pas et pourquoi certains d'entre eux peuvent être limités. Comme indiqué ci-dessus et dans de précédents chapitres, l'utilisation des droits doit être rendue effective. L'automatisation ainsi que les autres fonctionnalités des plateformes de médias sociaux devraient être utilisées pour faciliter l'exercice des droits.

b. Dispositions juridiques pertinentes

143. Le RGPD décrit sept droits différents que les personnes concernées peuvent exercer selon certaines conditions (par exemple, la base juridique du traitement, etc.). L'article 15 du RGPD permet aux personnes concernées de savoir si des données à caractère personnel les concernant sont traitées et d'avoir accès à ces données, c'est-à-dire d'obtenir de plus amples informations sur leur traitement, ainsi que de recevoir une copie de ces données. L'article 16 du RGPD précise le droit de rectification permettant aux personnes concernées de mettre à jour les données à caractère personnel traitées par le responsable du traitement. Le droit à l'effacement prévu à l'article 17 du RGPD permet aux personnes concernées d'obtenir l'effacement de données à caractère personnel les concernant. Le droit à la limitation du traitement prévu à l'article 18 du RGPD donne aux personnes concernées la possibilité d'interrompre temporairement le traitement de leurs données à caractère personnel. L'article 20 du RGPD introduit le droit à la portabilité des données, qui permet aux personnes concernées de recevoir leurs données à caractère personnel et de les transmettre à un autre responsable du traitement[68]. Les personnes concernées ont également le droit de s'opposer au traitement de leurs données à caractère personnel, comme le prévoit l'article 21 du RGPD. Enfin, l'article 22 du RGPD confère aux personnes concernées le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé[69].

144. L'EDPB souligne que ces droits ne s'appliqueront pas tous à chaque plateforme de médias sociaux; leur applicabilité dépend de la base juridique et des finalités de traitement des données à caractère personnel de la plateforme, ainsi que des types de services fournis. Les différences devraient être expliquées par le responsable du traitement conformément à l'article 12 du RGPD. Cela signifie que les informations relatives aux droits applicables, y compris les raisons pour lesquelles certains droits ne s'appliquent pas, devraient être concises et claires pour l'utilisateur. Une telle explication pourrait limiter le volume des communications avec l'utilisateur lorsqu'il tente d'exercer certains de ces droits. L'exercice du droit devrait être aisé et accessible, conformément à l'article 12, paragraphe 2, et la réponse devrait être donnée dans les meilleurs délais, comme l'exige l'article 12, paragraphe 3, du

[67] Lignes directrices sur le droit à la portabilité des données et lignes directrices 05/2019 sur les critères du droit à l'oubli au titre du RGPD dans le cadre des moteurs de recherche (partie 1) - version adoptée après consultation publique, disponibles à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_fr

[68] Ce droit est décrit plus en détail dans les lignes directrices sur le droit à la portabilité des données.

[69] Voir également les lignes directrices du groupe de travail «Article 29» relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, wp251rev.01, p. 19 et suivantes: https://ec.europa.eu/newsroom/article29/items/612053/en

RGPD. De même, la plateforme de médias sociaux devrait expliquer les raisons pour lesquelles il ne peut être donné suite à certaines demandes et informer l'utilisateur de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle désignée, conformément à l'article 12, paragraphe 4, du RGPD. Par conséquent, il est possible que les interfaces trompeuses suivantes ne s'appliquent pas à tous les droits susmentionnés. Le droit à l'effacement est abordé de façon détaillée dans le chapitre suivant.

c. Interfaces trompeuses

i. Interfaces trompeuses fondées sur le contenu

Obstruction – Impasse (annexe I, liste de contrôle 4.4.1)

145. L'interface trompeuse de type ***impasse*** peut avoir une incidence directe sur la facilité d'accès à l'exercice des droits. Lorsque les liens redirigeant vers les moyens d'exercer un droit sont défectueux ou en l'absence d'explications claires sur la manière d'exercer un droit, l'utilisateur n'est pas en mesure d'exercer ce droit de façon appropriée, ce qui constitue une violation de l'article 12, paragraphe 2, du RGPD.

> **Example 44:** l'utilisateur clique sur l'option «*exercer mon droit d'accès*» dans la déclaration de confidentialité, mais est redirigé vers son profil, qui ne propose aucune fonctionnalité liée à l'exercice de ce droit.

146. L'exemple d'interface trompeuse susmentionné souligne la nécessité de proposer à l'utilisateur une manière claire et intuitive d'exercer ses droits conformément à l'article 12, paragraphes 1 et 2, du RGPD, à défaut de quoi, il pourrait ne pas être en mesure de les exercer. Il ne suffit pas de confirmer à l'utilisateur qu'il dispose des droits conférés à la personne concernée, conformément à l'article 12, paragraphe 1, du RGPD (y compris la manière de communiquer) et, en particulier, à l'article 13, paragraphe 2, point b), et à l'article 14, paragraphe 2, point c), du RGPD. L'utilisateur doit aussi être en mesure d'exercer facilement ces droits, de préférence par un moyen intégré dans l'interface de la plateforme, par exemple un formulaire spécifique. Cela rendrait également l'expérience utilisateur sur la plateforme plus positive – le fournisseur ayant fait l'effort de s'adapter aux attentes de l'utilisateur, c'est-à-dire un traitement licite de ses données à caractère personnel et le contrôle sur ses données, en combinant l'exercice des droits avec d'autres fonctionnalités du service. Lorsque le service de la plateforme de médias sociaux permet une communication bidirectionnelle entre les utilisateurs, ainsi qu'entre le responsable du traitement et les utilisateurs, il n'y a aucune raison pour que le responsable du traitement limite son canal de communication prévu pour gérer les demandes des personnes concernées à un moyen de communication distinct tel que le courrier électronique. Dans le même temps, la personne concernée ne devrait pas être obligée de se rendre sur la plateforme pour communiquer avec le responsable du traitement[70]. En outre, les responsables du traitement ne peuvent limiter le droit de cette personne concernée d'obtenir une copie, mais doivent également veiller à fournir les informations visées à l'article 15, paragraphe 1, du RGPD à l'utilisateur qui demande l'accès à ses données[71].

[70] Voir les lignes directrices 01/2022 sur les droits des personnes concernées – droit d'accès, point 136, version 1.0, disponibles à l'adresse suivante: https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf

[71] Voir les lignes directrices 01/2022 de l'EDPB, points 131, 142 et 145.

Inconstance – Discontinuité linguistique (annexe I, liste de contrôle 4.5.4)

> **Example 45:** les informations que reçoit l'utilisateur lorsqu'il clique sur un lien en rapport avec l'exercice des droits des personnes concernées ne sont pas présentées dans la langue officielle de son pays, contrairement au service. Au lieu de cela, l'utilisateur est redirigé vers une page en anglais.

147. Compte tenu du principe de transparence énoncé à l'article 5, paragraphe 1, point a), et à l'article 12, paragraphe 1, du RGPD, toutes les informations relatives aux droits doivent être fournies à l'utilisateur d'une façon compréhensible, en des termes clairs et simples. Les informations doivent également être fournies en fonction de la localisation de l'utilisateur et de la langue utilisée dans le pays ou la juridiction dans lesquels le service est proposé. Le fait que l'utilisateur confirme être capable de communiquer dans une langue étrangère de quelque manière que ce soit ne dispense pas le responsable du traitement de ses obligations. Il en va de même lorsqu'il peut être déduit des activités de l'utilisateur qu'il possède une telle connaissance d'autres langues. Les informations devraient être pertinentes et utiles à l'utilisateur aux fins de l'exercice de ses droits.

Brouillage – Formulations ou informations ambigües (annexe I, liste de contrôle 4.6.3)

148. Dans le cadre des droits des personnes concernées, l'utilisateur peut également être confronté à l'interface trompeuse de type ***formulations ou informations ambiguës***, illustrée dans l'exemple suivant.

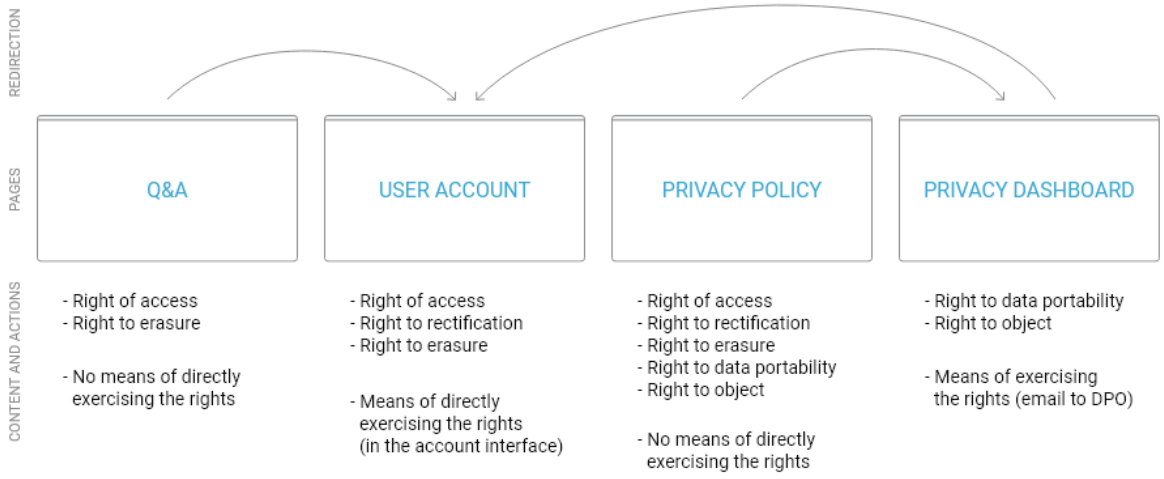
> **Example 46:** la plateforme de médias sociaux n'indique pas explicitement que les utilisateurs dans l'UE ont le droit d'introduire une réclamation auprès d'une autorité de contrôle, mais mentionne seulement que, dans certains pays (sans préciser lesquels), il existe des autorités chargées de la protection des données avec lesquelles le fournisseur de médias sociaux coopère en ce qui concerne les réclamations.

149. Les fournisseurs de médias sociaux doivent également veiller à éviter l'interface trompeuse de type ***formulations ou informations ambiguës*** lorsqu'ils informent la personne concernée de ses droits. Le fait d'informer l'utilisateur d'une manière qui ne lui permet pas de savoir avec certitude comment ses données seront traitées ou comment il peut exercer un certain contrôle sur ses données et, ainsi, exercer ses droits constitue une violation du principe de transparence. En outre, une formulation vague ne constitue pas un langage concis, comme l'exige l'article 12, paragraphe 1, du RGPD, et peut rendre incomplètes les informations fournies à la personne concernée, ce qui pourrait être considéré comme une violation de l'article 13 du RGPD. L'exemple susmentionné met également en évidence une violation de l'article 13, paragraphe 2, point d), du RGPD, qui impose au responsable du traitement de fournir à la personne concernée des informations sur son droit d'introduire une réclamation auprès d'une autorité de contrôle. Par extension, cela est également contraire à l'article 12, paragraphe 2, du RGPD, car le fournisseur de médias sociaux ne facilite pas l'exercice du droit d'introduire une réclamation.

ii. Interfaces trompeuses fondées sur le processus de navigation

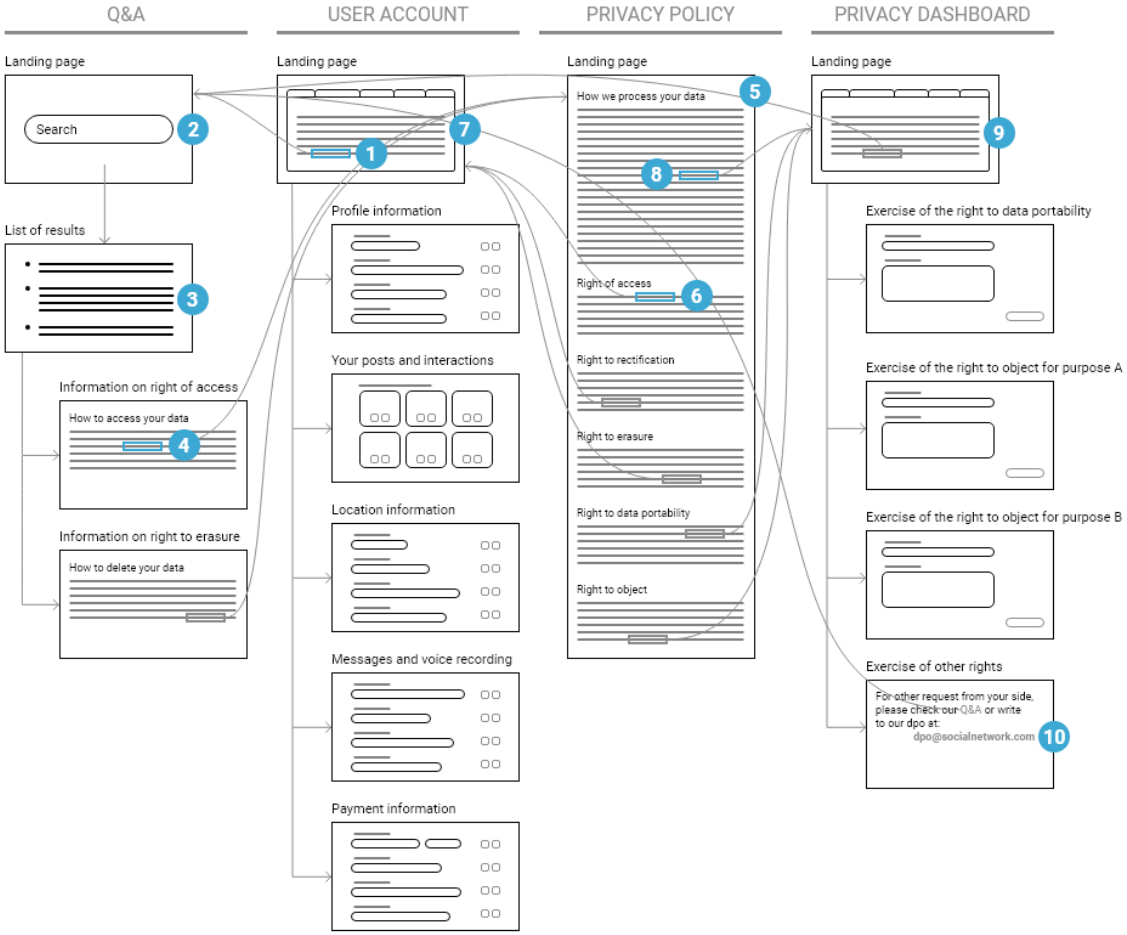
Surcharge – Labyrinthe (annexe I, liste de contrôle 4.1.2)

150. Comme décrit précédemment, dans le cas d'utilisation 3b, le nombre d'actions requises pour obtenir les informations utiles sur la protection des données ne doit pas être excessif, tout comme le nombre d'actions que la personne concernée doit exécuter pour exercer ses droits[72]. L'utilisateur devrait donc toujours pouvoir atteindre rapidement l'endroit où il peut exercer ses droits, quel que soit son point de départ et l'endroit de la plateforme de médias sociaux où se trouve cette fonctionnalité. Les fournisseurs de médias sociaux devraient donc réfléchir soigneusement aux différents cas dans lesquels l'utilisateur souhaite exercer ses droits et déterminer en conséquence l'accès à l'endroit où il peut les exercer. Cela signifie que plusieurs chemins d'accès aux droits d'une personne concernée peuvent être créés et proposés sur une plateforme de médias sociaux. Toutefois, chaque chemin devrait faciliter l'accès à l'exercice des droits et ne devrait pas interférer avec un autre. Dans le cas contraire, il serait considéré comme une interface trompeuse de type ***labyrinthe***, telle qu'illustrée par les exemples 47 et 48, contraire à l'article 12, paragraphe 2, du RGPD.



Example 47: dans ce cas précis, les informations concernant les droits relatifs à la protection des données sont réparties sur au moins quatre pages. Bien que la politique de confidentialité fournisse des informations sur tous les droits, elle ne redirige pas vers les pages pertinentes pour chacun d'entre eux. À l'inverse, lorsque l'utilisateur consulte son compte, il ne trouve aucune information sur certains des droits qu'il peut exercer. Ce ***labyrinthe*** l'oblige à explorer de nombreuses pages pour trouver où exercer chaque droit et, en fonction de sa navigation, il pourrait ne pas avoir connaissance de tous les droits dont il dispose.

[72] Voir point 123 ci-dessus.



Example 48: dans cet exemple, l'utilisateur souhaite mettre à jour certaines de ses données à caractère personnel mais ne trouve pas de moyen de le faire dans son compte. Il clique sur un lien (1) qui le redirige vers la section des questions et réponses, où il saisit sa question (2). Plusieurs résultats apparaissent (3), dont certains concernent les droits d'accès et de suppression. Après avoir vérifié tous les résultats, il clique (4) sur le lien proposé sur la page «Comment accéder à vos données». Ce lien le redirige vers la politique de confidentialité (5). L'utilisateur y trouve des informations sur d'autres droits. Après avoir lu ces informations, il clique (6) sur le lien associé à l'exercice du droit de rectification, qui le redirige vers le compte utilisateur (7). Insatisfait, il retourne à la politique de confidentialité et clique sur un lien général intitulé «Envoyer une demande» (8). Ce lien le conduit à son tableau de bord de la vie privée (9). Étant donné qu'aucune des options disponibles ne semble correspondre à ce qu'il cherche, l'utilisateur finit par se rendre sur la page «Exercice d'autres droits» (10), où il trouve enfin une adresse de contact.

151. Ces deux exemples illustrent des chemins particulièrement longs et fastidieux pour exercer ses droits. Lorsque les moyens d'exercer différents droits ne se trouvent pas au même endroit mais qu'une page énumérant tous les droits conférés à la personne concernée est disponible, cette dernière devrait rediriger précisément vers ces différents endroits, et pas seulement vers un ou une partie d'entre eux, comme l'illustre l'exemple 47. L'autre exemple illustre un parcours dans lequel l'utilisateur ne trouve

pas le moyen d'exercer facilement le droit spécifique qu'il souhaite, à savoir le droit de rectification, car l'endroit où il est habituellement exercé, c'est-à-dire le compte utilisateur, ne lui donne pas le moyen de le faire. Il cherche un autre moyen d'exercer ce droit mais n'en trouve pas de spécifique et doit se rabattre sur un moyen général fourni dans le tableau de bord de la vie privée.

152. Lorsque plusieurs chemins d'accès à l'exercice d'un droit ont été créés, l'utilisateur devrait toujours pouvoir consulter aisément la vue d'ensemble des droits des personnes concernées. La politique de confidentialité devrait être claire et pourrait servir de moyen, parmi d'autres, pour accéder aux pages où l'utilisateur peut exercer ses droits. Ce document devrait inclure tous les droits applicables. Si l'un d'entre eux ne s'applique pas en raison de limitations juridiques ou techniques, cela devrait également être expliqué, afin que l'utilisateur soit dûment informé. Il n'est pas seulement utile à l'utilisateur de comprendre les limites des opérations de traitement, que ce soit en raison de leur fondement ou des garanties adoptées par les responsables du traitement. Cela permet également de limiter les cas dans lesquels le fournisseur de médias sociaux doit expliquer les raisons pour lesquelles il ne peut donner suite à la demande d'un utilisateur concernant les droits des personnes concernées.

Incitation – Caché au grand jour (annexe I, liste de contrôle 4.3.2)

153. Il est également possible d'entraver la capacité de l'utilisateur à atteindre l'endroit où il peut exercer ses droits en rendant les informations ou les liens connexes difficilement visibles au moyen d'une interface trompeuse de type ***caché au grand jour***.

> **Example 49:** le paragraphe du sous-titre «droit d'accès» de la politique de confidentialité explique que l'utilisateur a le droit d'obtenir les informations visées à l'article 15, paragraphe 1, du RGPD. Toutefois, il mentionne uniquement la possibilité pour l'utilisateur d'obtenir une copie de ses données à caractère personnel. Il ne propose aucun lien direct visible permettant d'exercer la partie «copie» du droit d'accès prévu à l'article 15, paragraphe 3, du RGPD. Au lieu de cela, les trois premiers mots de la phrase «Vous pouvez obtenir une copie de vos données à caractère personnel» sont légèrement soulignés. Lorsque l'utilisateur passe la souris sur ces mots, une petite boîte contenant un lien vers les paramètres s'affiche.

154. Comme indiqué dans la section précédente, tout moyen créé par le responsable du traitement en vue de l'exercice des droits devrait être aisément accessible. Cette règle est incontournable. Une action du responsable du traitement telle que celle décrite ci-dessus ne peut être considérée que comme une initiative de sa part visant à entraver l'exercice de ses droits par l'utilisateur, ce qui constitue une violation de l'article 12, paragraphe 2, du RGPD. Les responsables du traitement, quelles que soient leurs raisons, ne devraient pas entraver une telle demande. Après un examen plus approfondi par une autorité de contrôle, dans certains cas, il pourrait s'agir d'une violation du RGPD entraînant une sanction à l'encontre du responsable du traitement.

Inconstance – Interface incohérente (annexe I, liste de contrôle 4.5.3)

> **Example 50:** la plateforme de médias sociaux propose différentes versions (bureau, application, navigateur mobile). Dans chaque version, les paramètres (donnant accès/objection, etc.) sont représentés par un symbole différent, ce qui est source de confusion pour l'utilisateur qui passe d'une version à une autre.

155. Confronté à des interfaces qui transmettent les mêmes informations par l'intermédiaire de signifiants visuels différents selon l'appareil utilisé, l'utilisateur mettra probablement davantage de temps ou aura davantage de difficultés à retrouver les outils de contrôle qu'il connaît lorsqu'il passe d'un appareil à un autre. Dans l'exemple ci-dessus, ces difficultés sont dues à l'utilisation de symboles ou d'icônes différents pour orienter l'utilisateur vers les paramètres. Le fait de semer ainsi la confusion dans l'esprit de l'utilisateur pourrait être considéré comme allant à l'encontre de la facilitation des droits conférés à la personne concernée prévue à l'article 12, paragraphe 2, du RGPD.

Obstruction – Processus plus long que nécessaire (annexe I, liste de contrôle 4.4.2)

156. Enfin, toute tentative de rendre le processus d'exercice d'un droit ***plus long que nécessaire*** peut être considérée comme contraire au RGPD.

> **Example 51:** lorsque l'utilisateur choisit de supprimer le nom et l'adresse de son lycée ou la référence à un événement auquel il a participé et qu'il a partagé, une deuxième fenêtre l'invitant à confirmer ce choix apparaît («*Voulez-vous vraiment faire cela? Pourquoi voulez-vous faire cela?*»).

157. Comme le nombre de niveaux dans une politique de confidentialité (cas d'utilisation 2a) et le nombre d'actions requises pour atteindre ou modifier un paramètre (cas d'utilisation 3b), le nombre d'actions ou de clics que l'utilisateur doit effectuer pour exercer un droit ne devrait pas être excessif. Cela dépend bien entendu de la complexité des opérations effectuées par le responsable du traitement, eu égard au contexte spécifique. Il serait toutefois déraisonnable d'exiger de l'utilisateur qu'il exécute un grand nombre d'actions inutiles pour mener à bien l'exercice de son droit. Par exemple, l'utilisateur ne devrait pas être découragé par des questions supplémentaires, telles que la question de savoir s'il souhaite réellement exercer ce droit ou quelles sont les raisons d'une telle demande. Dans la plupart des cas, il devrait pouvoir simplement exercer son droit, sans que sa motivation soit remise en question. De telles pratiques, illustrées dans l'exemple ci-dessus, peuvent être considérées comme contraires à l'article 12, paragraphe 2, du RGPD, dès lors que le responsable du traitement entrave l'exercice des droits par des actions inutiles. Naturellement, cela n'empêche pas le responsable du traitement de demander l'avis de l'utilisateur en lui posant ensuite des questions supplémentaires dans le but d'améliorer le service. Si cette question est posée a posteriori, la réponse dépendra exclusivement du bon vouloir de l'utilisateur et ne sera pas confondue avec une obligation aux fins de l'exercice d'un droit.

d. Bonnes pratiques

Formulaire d'exercice des droits: pour permettre à l'utilisateur d'exercer facilement les droits que lui confère le RGPD, fournir un formulaire spécifique qui l'aide à comprendre ses droits et lui indique la marche à suivre pour effectuer ces types de demandes.

Raccourcis: pour la définition, voir le cas d'utilisation n° 1 (p. 22) (*par exemple, fournir un lien vers la suppression du compte dans le compte d'utilisateur*).

Formulation cohérente: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Fournir des définitions: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Utilisation d'exemples: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Navigation «collée»: pour la définition, voir le cas d'utilisation n° 2a (p. 28).

Expliquer les conséquences: pour la définition, voir le cas d'utilisation n° 2c (p. 32)**.**

Cohérence entre les différents appareils: pour la définition, voir le cas d'utilisation n° 3a (p. 39).

Répertoire de la protection des données: pour la définition, voir le cas d'utilisation n° 3b (p. 45).

Lien entre les outils de contrôle de la protection des données: pour la définition, voir le cas d'utilisation n° 3b (p. 45).

3.5 Au revoir et adieu: quitter un compte sur les médias sociaux

Cas d'utilisation n° 5: suspension du compte/effacement de toutes les données à caractère personnel

a. Description du contexte et des dispositions juridiques pertinentes

158. La fin du cycle de vie d'un compte correspond au moment où l'utilisateur décide de quitter le réseau social. Dans cette situation, l'utilisateur décide généralement de quitter la plateforme de médias sociaux de manière définitive. Toutefois, il est souvent possible également de désactiver le compte et de suspendre le service seulement de façon temporaire. Les deux décisions ont des conséquences différentes, décrites ci-après.

i. Effacement définitif du compte

159. La décision de quitter définitivement la plateforme de médias sociaux s'accompagne du droit à l'effacement prévu à l'article 17, paragraphe 1, point a), du RGPD. Dans ce contexte, on parle plus souvent de «suppression» que d'«effacement».

160. Le terme «effacement» n'est pas défini juridiquement à l'article 17 du RGPD et n'est mentionné qu'en tant que forme de traitement à l'article 4, point 2, du RGPD. Le terme «effacement» s'entend généralement comme l'impossibilité (matérielle) d'apercevoir les informations relatives à une personne concernée qui figuraient précédemment dans les données à effacer. Après l'effacement, il ne doit plus être possible pour quiconque d'apercevoir les informations en question sans effort disproportionné.

161. L'anonymisation est un autre moyen de supprimer définitivement le lien avec une personne. En d'autres termes, l'utilisation de techniques d'anonymisation vise à garantir que la personne concernée n'est plus identifiable. L'anonymisation signifie également que les principes de la législation en matière de protection des données (tels que le principe de limitation des finalités) ne s'appliquent plus (voir considérant 26, quatrième et cinquième phrases).

162. Aux termes de l'article 12, paragraphe 2, du RGPD, le responsable du traitement facilite l'exercice des droits conférés à la personne concernée au titre des articles 15 à 22. Selon cette exigence, il ne peut être créé aucun obstacle matériel ou formel à l'affirmation des droits des personnes concernées. Dès lors, si l'exercice du droit à l'effacement est rendu plus difficile sans raison valable, cela constitue une violation du RGPD. S'il existe une raison valable pour que les fournisseurs de médias sociaux expliquent objectivement les conséquences, telles que la suppression de toutes les données à caractère personnel, et demandent aux personnes concernées de confirmer ce choix[73], il convient également d'éviter les obstacles inutiles dans le présent cas d'utilisation. Il en découle, par exemple, que tout

[73] Contrairement aux autres droits des personnes concernées, voir point 154 ci-dessus.

délai de grâce entre la demande de suppression du compte d'un utilisateur et la suppression effective du compte doit être proportionné. Ainsi, ce délai ne peut pas être excessif, tout en tenant compte des nécessités techniques justifiant de ne pas procéder immédiatement à la suppression, ainsi que d'un court délai pour permettre à l'utilisateur de reconsidérer la suppression de son compte une fois qu'il a enclenché le processus. Si l'utilisateur doit être libre de changer d'avis, les fournisseurs de médias sociaux ne doivent pas essayer de provoquer un tel changement en incitant l'utilisateur à revenir en arrière, ce qui constituerait également une entrave au droit de suppression de l'utilisateur. Pendant le délai de grâce, le processus de suppression peut être interrompu dans certains cas, par exemple lorsque l'utilisateur se connecte à nouveau. Si la suppression n'est pas possible, il convient d'en informer l'utilisateur et de lui indiquer la manière de procéder pour effectuer cette suppression.

163. La décision de quitter la plateforme de médias sociaux a pour conséquence l'effacement, comme indiqué à l'article 17, paragraphe 1, du RGPD. Si une personne concernée demande la suppression de son compte, le responsable du traitement de la plateforme de médias sociaux doit supprimer les données. Néanmoins, certaines données peuvent être conservées sur la plateforme pendant un certain temps si l'article 17, paragraphe 3, du RGPD s'applique. Les exceptions énumérées à l'article 17, paragraphe 3, du RGPD doivent être interprétées de manière restrictive et ne s'appliquent que dans les cas expressément cités dans cette partie de la disposition. Toute exception invoquée par un responsable du traitement en vertu de l'article 17, paragraphe 3, du RGPD et la conservation des données qui en découle doivent être justifiées par le responsable du traitement, par exemple par le fait que le droit national lui impose de stocker des informations relatives à la personne concernée pour des raisons impérieuses d'intérêt public, aux fins de l'exercice du droit fondamental à la liberté d'expression et d'information, ou pour des raisons fiscales. Il va sans dire que les données ainsi conservées ne devraient être stockées qu'en interne par le fournisseur de médias sociaux et ne devraient pas être visibles par d'autres utilisateurs. Toutefois, une exception au titre de l'article 17, paragraphe 3, du RGPD ne permet en aucun cas au fournisseur de médias sociaux de continuer d'administrer le compte de la personne concernée plus longtemps que ce qu'avait prévu l'utilisateur après sa demande de suppression.

164. Indépendamment de toute demande de suppression de compte, si l'utilisateur retire son consentement en vertu de l'article 7, paragraphe 3, du RGPD, le traitement des données qu'il a communiquées par consentement conformément à l'article 6, paragraphe 1, point a), du RGPD ne peut plus avoir lieu. Dans ce cas, d'autres opérations de traitement pour lesquelles le fournisseur de médias sociaux se fonde sur d'autres bases juridiques en vertu de l'article 6, paragraphe 1, du RGPD peuvent, dans certaines circonstances, encore avoir lieu.

165. Toutefois, si l'utilisateur demande la suppression de son compte, aucun traitement ultérieur ne devrait être mis en œuvre, quelle que soit la base juridique invoquée, sauf si l'une des exceptions citées dans la liste exhaustive de l'article 17, paragraphe 3, du RGPD s'applique. Dans ce contexte, il importe de garder à l'esprit que la conservation est limitée au stockage minimal susmentionné.

166. Selon l'article 25, paragraphe 1, du RGPD, le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées afin de mettre en pratique les principes relatifs à la protection des données. Selon les lignes directrices 04/2019 relatives à l'article 25 – Protection des données dès la conception et protection des données par défaut, les mesures techniques et organisationnelles peuvent s'entendre au sens large comme toute méthode ou tout moyen qu'un responsable du traitement peut employer dans le cadre du traitement. *Approprié* signifie que les mesures doivent être adaptées pour atteindre le but visé, c'est-à-dire qu'elles doivent mettre en

œuvre les principes de protection des données de façon effective. Ainsi, l'exigence du caractère approprié est étroitement liée à l'exigence d'effectivité[74].

[74] Lignes directrices 04/2019 relatives à l'article 25 – Protection des données dès la conception et protection des données par défaut, p. 6, point 8.

ii. Suspension du compte

167. L'utilisateur a également la possibilité de désactiver temporairement son compte, ce qui lui permet de quitter le média social pendant un certain temps sans supprimer son compte de manière définitive. Dans ce cas, le compte est temporairement désactivé et le profil, les images, les commentaires et les réactions seront cachés jusqu'à ce que l'utilisateur réactive son compte, par exemple en se reconnectant. La principale différence avec l'effacement réside dans le fait que les données à caractère personnel sont conservées dans le réseau social et que l'utilisateur peut réactiver son compte sans devoir se réinscrire.

168. Lorsqu'un utilisateur entame le processus de suppression de son compte, il constate parfois que c'est l'option de suspension de compte qui est sélectionnée par défaut. Si une telle option peut être utile pour l'utilisateur qui ne souhaite pas encore supprimer définitivement son compte, le fournisseur de médias sociaux ne peut pas imposer de tels délais de réflexion aux utilisateurs, surtout par défaut. En se voyant offrir la possibilité de désactiver son compte, l'utilisateur s'attend raisonnablement à ce que ses données à caractère personnel ne soient pas traitées de la même manière que pendant l'utilisation active de son compte, et à ce que le fournisseur réduise le traitement de ses données à caractère personnel au strict nécessaire pendant cette période. L'utilisateur peut s'attendre à ce que ses données ne soient pas traitées, ou pas entièrement, à des fins spécifiques, par exemple en optimisant son profil grâce à des visites sur des sites internet tiers qui utilisent des outils de ciblage ou de suivi appropriés. Outre le fait de communiquer à l'utilisateur des informations sur les conséquences de la suspension de son compte de manière transparente, tout traitement de données effectué pendant cette suspension doit être fondé sur une base juridique valable.

169. En ce qui concerne le traitement des données fondé sur le consentement conformément à l'article 6, paragraphe 1, point a), du RGPD, le fournisseur de médias sociaux doit tenir compte du fait que l'utilisateur s'attend à ce que le consentement qu'il donne lors de son inscription ou ultérieurement couvre uniquement le traitement de ses données pendant l'utilisation active de son compte. L'EDPB reconnaît que la durée du consentement dépend du contexte, de la portée du consentement initial et des attentes de la personne concernée[75]. Bien que le RGPD ne fixe pas de durée spécifique pendant laquelle le consentement restera valable, la durée de validité de celui-ci dépendra du contexte, de la portée du consentement initial et des attentes de la personne concernée[76]. Si les opérations de traitement changent ou évoluent considérablement, le consentement initial n'est plus valable[77]. L'EDPB recommande, à titre de meilleure pratique, que le consentement soit renouvelé à des intervalles appropriés[78]. Fournir à nouveau toutes les informations permet de garantir que la personne concernée demeure bien informée de la façon dont ses données sont utilisées et dont elle peut exercer ses droits[79]. Dans ce cas, un nouveau consentement doit être obtenu[80] et toutes les exigences correspondantes doivent être satisfaites.

170. Les attentes raisonnables de la personne concernée devraient également être prises en considération lorsque l'article 6, paragraphe 1, point f), du RGPD est applicable (voir considérant 47). En particulier, il convient de déterminer si la personne concernée peut raisonnablement s'attendre, au moment de la collecte des données à caractère personnel et dans le cadre de celle-ci, à ce qu'un traitement à cette fin puisse avoir lieu. Or, l'utilisateur s'attend raisonnablement à ce que seul le traitement de données

[75] Lignes directrices 05/2020 sur le consentement, point 110.
[76] Lignes directrices 05/2020 sur le consentement, point 110.
[77] Lignes directrices 05/2020 sur le consentement, point 110.
[78] Lignes directrices 05/2020 sur le consentement, point 111.
[79] Lignes directrices 05/2020 sur le consentement, point 111.
[80] Voir les lignes directrices 05/2020 sur le consentement, point 110.

nécessaire ait lieu pendant la période de désactivation. En outre, le fournisseur de médias sociaux ne peut invoquer un intérêt légitime que si toutes les conditions du critère de l'intérêt légitime, y compris l'exercice de mise en balance, sont satisfaites. L'intérêt supérieur ou les droits et libertés fondamentaux de la personne concernée devraient être appréciés au cas par cas.

171. Étant donné que les obligations contractuelles sont également suspendues dans une large mesure pendant la période de désactivation, les opérations de traitement des données ne sont nécessaires que dans la mesure limitée prévue à l'article 6, paragraphe 1, point b), du RGPD. Seul le stockage des données de l'utilisateur jusqu'à la décision finale de réactivation ou de suppression peut être considéré comme nécessaire.

172. Étant donné que tous les traitements de données antérieurs concernaient un compte actif, il convient de fournir des informations supplémentaires sur le traitement pendant la désactivation si elles ne figurent pas dans les informations générales visées aux articles 13 et 14 du RGPD. Cela découle des principes de transparence et de loyauté énoncés à l'article 5, paragraphe 1, point a), du RGPD et du principe de limitation des finalités énoncé à l'article 5, paragraphe 1, point b), du RGPD. Le traitement des données à la suite de la désactivation doit être accompagné d'une information suffisante de la personne concernée. Par conséquent, le fournisseur de médias sociaux informera l'utilisateur de manière exhaustive du traitement effectif et de ses finalités pendant la suspension et, si nécessaire, demandera à nouveau son consentement.

b. Interfaces trompeuses

i. Interfaces trompeuses fondées sur le contenu

Surcharge – Labyrinthe (annexe I, liste de contrôle 4.1.2)

173. Dans le présent cas d'utilisation, l'interface trompeuse de type ***labyrinthe*** réside dans le fait de noyer l'utilisateur sous une masse d'informations, disséminées à plusieurs endroits, afin de l'empêcher de supprimer son compte, comme le montre l'exemple ci-dessous. Bien que certaines informations supplémentaires avant cette étape soient tout à fait souhaitables, comme le fait d'indiquer à l'utilisateur qu'il a accès à ses données avant la suppression de son compte, les informations générales non pertinentes ne sont plus essentielles. Il convient de ne pas freiner inutilement l'utilisateur dans cette démarche.

> **Example 52:** l'utilisateur cherche le droit à l'effacement. Il doit consulter les paramètres du compte, ouvrir un sous-menu intitulé «protection de la vie privée» et le dérouler jusque tout en bas pour trouver un lien lui permettant de supprimer son compte.

Incitation – Pilotage émotionnel (annexe I, liste de contrôle 4.3.1)

> **Example 53:** au premier niveau d'information, les informations fournies à l'utilisateur ne mettent en évidence que les conséquences négatives, qui le dissuadent de supprimer son compte (par exemple, «*vous perdrez tout de manière définitive*» ou «*vos amis vont vous oublier*»).

174. Alors que le fait de regretter la fin d'une relation contractuelle semble socialement acceptable et est donc difficile à saisir en termes juridiques, une description complète des conséquences prétendument négatives de la suppression de son compte par l'utilisateur constitue un obstacle à sa décision si elle est faite comme dans l'exemple ci-dessus, qui joue sur la peur de manquer quelque chose, donnant

l'impression que le choix de supprimer son compte est particulièrement punitif. Un tel ***pilotage émotionnel,*** dans le cadre duquel l'utilisateur est menacé de se retrouver seul s'il supprime son compte, constitue une violation de l'obligation de faciliter l'exercice des droits conférés à la personne concernée prévue à l'article 12, paragraphe 2, du RGPD, ainsi que du principe de loyauté énoncé à l'article 5, paragraphe 1, point a), du RGPD.

Brouillage – Formulations ou informations ambigües (annexe I, liste de contrôle 4.6.3)

175. Lors de la suppression d'un compte sur les médias sociaux, l'utilisateur peut également être confronté à l'interface trompeuse de type ***formulations ou informations ambiguës***, telle qu'illustrée dans l'exemple suivant.

> **Example 54:** lorsque l'utilisateur supprime son compte, il n'est pas informé de la durée pendant laquelle ses données seront conservées une fois le compte supprimé. Pire encore, à aucun moment dans le processus de suppression, il n'est informé du fait que «*certaines données à caractère personnel*» pourraient être conservées même après la suppression du compte. Il doit rechercher lui-même les informations auprès des différentes sources d'information disponibles.
>
> **Example 55:** l'utilisateur ne peut supprimer son compte que par les liens intitulés «*À bientôt*» ou «*Désactiver*» disponibles sur son compte.

176. Dans ces exemples, la formulation utilisée dans les liens n'indique pas clairement que l'utilisateur sera redirigé vers le processus de suppression de compte. Au lieu de cela, elle évoquera probablement pour l'utilisateur d'autres fonctionnalités, comme la déconnexion jusqu'à la prochaine utilisation ou la désactivation de son compte. Cela pourrait être interprété comme une violation de l'article 12, paragraphe 2, du RGPD, selon lequel les responsables du traitement devraient faciliter l'exercice des droits conférés à la personne concernée. En semant la confusion par rapport aux attentes de l'utilisateur associées au lien, la plateforme de médias sociaux ne facilite pas pleinement l'exercice du droit à l'effacement. L'utilisation de termes aussi équivoques dans un autre contexte pourrait constituer une violation de dispositions du RGPD telles que l'article 7 et, par extension, l'article 17, paragraphe 1, point b).

ii. Interfaces trompeuses fondées sur le processus de navigation

Inattention – Confort trompeur (annexe I, liste de contrôle 4.2.1)

> **Example 56:** lors de la suppression de son compte, l'utilisateur a le choix entre les deux options suivantes: supprimer son compte ou le suspendre. C'est l'option de suspension qui est sélectionnée par défaut.

177. La première option, c'est-à-dire la suppression du compte, entraîne la suppression de toutes les données à caractère personnel de l'utilisateur, ce qui signifie que la plateforme de médias sociaux n'est plus en possession de ces données, à l'exception des données relevant de l'exception temporaire prévue à l'article 17, paragraphe 3, du RGPD. En revanche, avec la deuxième option, c'est-à-dire la suspension du compte, toutes les données à caractère personnel sont conservées et susceptibles d'être traitées par le fournisseur de médias sociaux. Cette option présente nécessairement davantage de risques pour la personne concernée, par exemple si, à la suite d'une violation de données, les données toujours stockées par le fournisseur de médias sociaux sont consultées, reproduites,

transférées ou traitées de toute autre manière. La sélection par défaut de l'option de suspension incitera probablement l'utilisateur à sélectionner cette option plutôt que de supprimer son compte comme il le prévoyait initialement. Par conséquent, la pratique décrite dans cet exemple peut être considérée comme une violation de l'article 12, paragraphe 2, du RGPD, puisque, dans ce cas, elle ne facilite pas l'exercice du droit à l'effacement, et tente même d'empêcher l'utilisateur d'exercer ce droit.

Inattention – Détournement d'attention (annexe I, liste de contrôle 4.2.2)

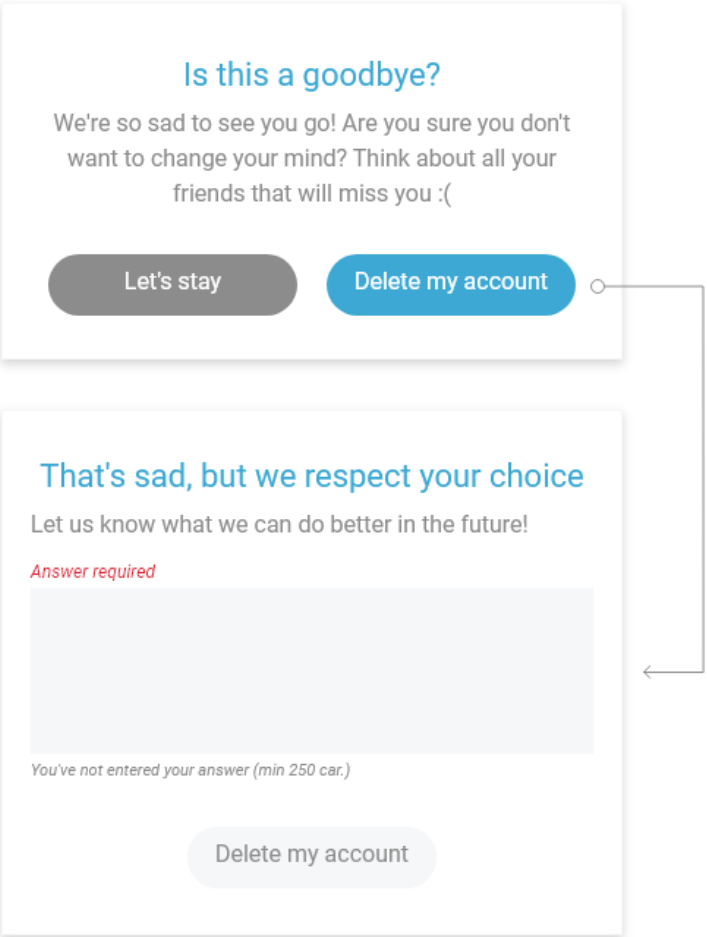
178. Il peut être utile de donner à l'utilisateur un moyen de télécharger ses données lorsqu'il exprime le souhait de supprimer son compte. En effet, une fois son compte supprimé, ses données à caractère personnel seront effacées après un certain laps de temps. Cela signifie que, s'il n'obtient pas une copie de ses données à caractère personnel, il les perdra à tout jamais. Toutefois, la présentation de cette option peut constituer une interface trompeuse de type ***détournement de l'attention***, comme le montre l'exemple suivant.

Example 57: après avoir cliqué sur «Supprimer mon compte», l'utilisateur se voit proposer la possibilité de télécharger ses données, en application du droit à la portabilité, avant de supprimer son compte. Lorsqu'il clique pour télécharger ses informations, il est redirigé vers une page d'information sur le téléchargement. Toutefois, une fois que l'utilisateur a choisi ce qu'il souhaite télécharger et le mode de téléchargement de ses données, il n'est pas redirigé vers le processus de suppression.

179. Dans l'exemple ci-dessus, on pourrait considérer que la manière dont l'option de téléchargement est mise en œuvre ne facilite pas l'exercice du droit à l'effacement associé à la suppression du compte. En effet, une fois que l'utilisateur a téléchargé ses données, il n'est pas redirigé vers le processus de suppression. Pour y revenir, il devra cliquer plusieurs fois. Entraver d'une telle manière l'exercice d'un droit constitue une violation de l'article 12, paragraphe 2, du RGPD. En outre, fournir un moyen d'atteindre facilement le processus de suppression après avoir téléchargé ses données est une fonctionnalité très simple à mettre en œuvre. À cet égard, il pourrait être considéré que l'obligation de mettre en œuvre des mesures techniques et organisationnelles appropriées prévue à l'article 25, paragraphe 1, du RGPD n'est pas respectée, dès lors que l'utilisateur n'est pas en mesure de continuer d'exercer ses droits de manière effective.

Obstruction – Processus plus long que nécessaire (annexe I, liste de contrôle 4.4.2)

180. Comme expliqué en détail dans le cas d'utilisation 4, toute action inutile ajoutée à l'exercice d'un droit pourrait enfreindre les dispositions du RGPD, en particulier l'article 12, paragraphe 2. Cela s'applique au moment où l'utilisateur cherche à supprimer son compte, car une telle pratique porterait atteinte au droit à l'effacement associé à sa demande.



Example 58: dans cet exemple, l'utilisateur voit d'abord s'afficher une boîte l'invitant à confirmer la suppression de son compte après avoir cliqué sur le lien ou le bouton correspondant dans son compte. Bien qu'un certain ***pilotage émotionnel*** soit à l'œuvre dans cette boîte, cette étape peut être considérée comme une mesure de sécurité destinée à éviter que l'utilisateur supprime son compte à la suite d'un clic erroné dans son compte. Toutefois, lorsque l'utilisateur clique sur le bouton «Supprimer mon compte», une deuxième boîte s'affiche, qui l'invite à décrire textuellement la raison pour laquelle il souhaite supprimer son compte. Tant qu'il n'a pas saisi du texte dans la boîte, il lui est impossible de supprimer son compte car le bouton associé à l'action est inactif et grisé. Cette pratique rend le processus d'effacement d'un compte ***plus long que nécessaire***, notamment parce que produire un texte décrivant les raisons pour lesquelles l'utilisateur souhaite quitter le réseau social nécessite davantage d'efforts et de temps, et ne devrait pas être obligatoire pour supprimer son compte.

181. Comme indiqué précédemment, lorsqu'il exerce un droit, l'utilisateur ne devrait pas avoir à répondre à des questions sans rapport avec l'exercice du droit lui-même. Le fait de devoir justifier son choix ou expliquer comment la plateforme de médias sociaux devrait s'améliorer ne relève pas de cette catégorie. Ce problème se pose de façon amplifiée dans l'exemple illustré, car la personne concernée doit rédiger une réponse au lieu de sélectionner une proposition prédéfinie dans une liste, ce qui est encore plus fastidieux pour elle puisqu'elle doit créer entièrement la réponse. Un tel mécanisme

pourrait empêcher certains utilisateurs d'exercer leur droit s'ils ne se sentent pas suffisamment à l'aise pour rédiger une réponse.

182. Toutefois, cela ne signifie pas qu'il soit acceptable d'ajouter au processus de suppression du compte une étape consistant en une liste de réponses prédéfinies. Cela est particulièrement vrai si ces réponses sont associées à d'autres étapes et actions imposées à l'utilisateur, comme l'illustre l'exemple ci-dessous.

> **Example 59:** le fournisseur de médias sociaux oblige l'utilisateur à répondre à une question sur les raisons pour lesquelles il souhaite supprimer son compte en choisissant parmi plusieurs réponses dans un menu déroulant. L'utilisateur pense que le fait de répondre à cette question lui permet (apparemment) de réaliser l'action qu'il souhaite, à savoir supprimer son compte. Une fois la réponse sélectionnée, une fenêtre contextuelle apparaît, indiquant à l'utilisateur comment résoudre le problème indiqué dans sa réponse. Le processus de questions-réponses ralentit donc l'utilisateur dans le processus d'effacement de son compte.

183. Outre le fait qu'il rend le processus particulièrement long, le mécanisme de ***détournement d'attention*** vise à détourner l'utilisateur de son intention de supprimer son compte en lui proposant une solution au problème qui a motivé sa décision de quitter la plateforme de médias sociaux. Cette pratique entrave l'exercice du droit à l'effacement et, par extension, dissuade les personnes concernées d'exercer leur droit.

Inconstance – Décontextualisation (annexe I, liste de contrôle 4.5.2)

184. Enfin, une interface trompeuse de type ***décontextualisation*** peut également survenir lorsque l'utilisateur souhaite supprimer son compte.

> **Example 60:** sur la plateforme de médias sociaux XY, le lien permettant de désactiver ou de supprimer le compte se trouve sous l'onglet «*Vos données XY*».

185. D'une manière générale, les termes utilisés pour intituler une page ou une section de la plateforme de médias sociaux consacrée aux questions de protection des données devraient refléter clairement le type d'informations ou d'outils de contrôle qui y figurent. Il est peu probable que l'utilisateur moyen associe les actions de suppression ou de désactivation de son compte à la gestion des données. Dans l'exemple précédent, l'utilisateur ne s'attend pas à trouver la fonctionnalité de suppression de son compte sur une page intitulée «Vos informations XY», qui fait allusion à la consultation et à l'éventuelle révision de ses informations. Il risque de chercher plutôt une page intitulée «Généralités» ou «Supprimer mon compte». Par conséquent, du point de vue de l'utilisateur, les options sont placées à un endroit qui est hors contexte et ne correspond pas à ses attentes.

> **Example 61:** l'onglet permettant effectivement de supprimer un compte se trouve dans la section «*supprimer une fonction de votre compte*».

186. Dans cet exemple, l'utilisateur peut comprendre par erreur le titre de la section comme indiquant simplement l'endroit où modifier différentes fonctions. Il ne s'attend donc pas à trouver là l'option permettant de supprimer l'ensemble de son compte. Dès lors, il est difficile pour l'utilisateur de trouver le lien correct pour supprimer l'intégralité de son compte.

187. L'interface trompeuse de type ***décontextualisation***, telle qu'illustrée dans les deux exemples ci-dessus, pourrait être considérée comme une violation de l'article 12, paragraphe 2, du RGPD, car l'utilisateur a du mal à trouver le bon endroit où exercer son droit à l'effacement.

c. Bonnes pratiques

Formulation cohérente: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Fournir des définitions: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Utilisation d'exemples: pour la définition, voir le cas d'utilisation n° 1 (p. 22).

Expliquer les conséquences: pour la définition, voir le cas d'utilisation n° 2c (p. 32).

Cohérence entre les différents appareils: pour la définition, voir le cas d'utilisation n° 3a (p. 39)**.**

Pour le comité européen de la protection des données

Le président

(Andrea Jelinek)

4 ANNEXE I: LISTE DES CATEGORIES ET TYPES D'INTERFACES TROMPEUSES

La liste suivante donne une vue d'ensemble des catégories d'interfaces trompeuses et des types d'interfaces trompeuses au sein de chaque catégorie. Elle énumère également les dispositions du RGPD les plus concernées selon les types d'interfaces trompeuses. Le lecteur devrait garder à l'esprit que, comme indiqué ci-dessus, le principe de traitement loyal énoncé à l'article 5, paragraphe 1, point a), du RGPD est le point de départ pour déterminer s'il existe des interfaces trompeuses. Il a une fonction générique et toutes les interfaces trompeuses ne le respecteraient pas, indépendamment du respect d'autres principes relatifs à la protection des données[81].

La liste indique également, pour chaque interface trompeuse, les références des exemples et des cas d'utilisation (CU) correspondants, afin d'aider le lecteur à les trouver rapidement.

Il importe de faire remarquer que cette liste n'est pas exhaustive et qu'il peut donc également exister des interfaces trompeuses dans des cas d'utilisation pour lesquels aucun exemple illustrant ce type d'interface trompeuse ne figure dans le texte des présentes lignes directrices.

4.1 Surcharge

Noyer l'utilisateur sous une masse de demandes, d'informations, d'options ou de possibilités afin de le dissuader d'aller plus loin et de l'inciter à conserver ou à accepter certaines pratiques en matière de données.

4.1.1 Incitation répétitive[82]

Inciter l'utilisateur à communiquer davantage de données à caractère personnel que ce qui est nécessaire aux fins du traitement ou à accepter une autre utilisation de ses données, en lui demandant à plusieurs reprises de fournir des données ou de consentir à une nouvelle finalité de traitement. Ces incitations répétitives peuvent survenir sur un ou plusieurs appareils. Il est probable que l'utilisateur finisse par céder, lassé de devoir refuser la demande chaque fois qu'il utilise la plateforme, ce qui le perturbe dans son utilisation.

Dispositions concernées du RGPD:

- *limitation des finalités: article 5, paragraphe 1, point b);*
- *consentement donné librement: article 7*, lu en combinaison avec l'article 4, point 11;
- *consentement spécifique: article 7, paragraphe 2.*

Exemples: cas d'utilisation (CU) n° 1, exemples 1 et 2; CU n° 3a, exemple 34 (illustration).

4.1.2 Labyrinthe

Lorsque l'utilisateur souhaite obtenir certaines informations, utiliser un outil de contrôle spécifique ou exercer un droit conféré à la personne concernée, il lui est particulièrement difficile de les trouver, car il doit naviguer sur un trop grand nombre de pages pour obtenir les

[81] Voir ci-dessus, point 9 des présentes lignes directrices.

[82] Cette interface trompeuse est étroitement liée à un type d'interface appelé «harcèlement», mentionné dans la littérature universitaire.

informations ou trouver l'outil de contrôle souhaités, sans disposer d'une vue d'ensemble complète et exhaustive. Il est probable que l'utilisateur abandonne ou passe à côté des informations ou de l'outil de contrôle recherchés.

Dispositions concernées du RGPD:

- *principe de transparence*: *article 5, paragraphe 1, point a), et transparence des informations: article 12, paragraphe 1;*
- *principe de loyauté: article 5, paragraphe 1, point a);*
- *informations aisément accessibles*: article 12, paragraphe 1;
- *accès aisé aux droits:* article 12, paragraphe 2;
- *consentement éclairé*: *article 7*, lu en combinaison avec l'article 4, point 11.

Exemples: CU n° 2a, exemple 17; CU n° 3a, exemple 33; CU n° 3b, exemple 37; CU n° 4, exemples 47 (illustration) et 48 (illustration); CU n° 5, exemple 51.

4.1.3 Trop nombreuses options

Proposer de (trop) nombreuses options à l'utilisateur. Face à de trop nombreuses options, l'utilisateur est incapable de faire un choix ou ne remarque pas certains paramètres, en particulier si aucune information ne lui est fournie. Cela peut le conduire à abandonner ou à passer à côté des paramètres relatifs à ses préférences ou à ses droits en matière de protection des données.

Dispositions concernées du RGPD:

- *principes de transparence et de loyauté:* article 5, paragraphe 1, point a);
- *transparence des informations*: article 12, paragraphe 1.

Exemple: CU n° 3b, exemple 35.

4.2 Inattention

Concevoir l'interface ou le parcours utilisateur de telle manière que l'utilisateur omet ou néglige tout ou partie des aspects liés à la protection des données.

4.2.1 Confort trompeur

Les fonctionnalités et options activées par défaut sont les plus intrusives. Compte tenu de l'effet «par défaut» qui pousse l'utilisateur à conserver une option par défaut, il est peu probable que celui-ci modifie cette option, même s'il en a la possibilité.

Dispositions concernées du RGPD:

- *protection des données dès la conception et protection des données par défaut*: article 25, paragraphe 1;
- *consentement:* article 4, paragraphe 11, et article 6 (pratique illégale consistant à activer par défaut un traitement fondé sur le consentement).

Exemples: CU n° 1, exemple 9; CU n° 3b, exemples 39 (illustration) et 40 (illustration); CU n° 5, exemple 55.

4.2.2 Détournement d'attention

Une action ou une information relative à la protection des données est mise en concurrence avec un autre élément qui peut être lié ou non à la protection des données. Lorsque l'utilisateur choisit cette option destinée à détourner son attention, il est probable qu'il oublie l'autre option, même s'il s'agit de celle qu'il avait l'intention de choisir au départ.

Dispositions concernées du RGPD:

- *principes de transparence et de loyauté:* article 5, paragraphe 1, point a);
- *transparence des informations*: article 12, paragraphe 1;
- *exercice des droits:* article 12, paragraphe 2.

Exemples: CU n° 2c, exemple 25; CU n° 3a, exemple 29; CU n° 5, exemples 56 et 58.

4.3 Incitation

Influencer le choix que ferait l'utilisateur en faisant appel à ses émotions ou en utilisant des indications visuelles.

4.3.1 Pilotage émotionnel[83]

Utiliser une formulation ou des éléments visuels (tels qu'un style, des couleurs, des images ou autres) de manière à transmettre des informations à l'utilisateur sous un jour soit très positif, en faisant en sorte qu'il se sente bien, en sécurité ou récompensé, soit très négatif, en faisant en sorte qu'il se sente angoissé, coupable ou sanctionné. Influer sur l'état émotionnel de l'utilisateur de cette manière risque de l'amener à exécuter une action allant à l'encontre de ses intérêts en matière de protection des données.

Dispositions concernées du RGPD:

- *principes de transparence et de loyauté:* article 5, paragraphe 1, point a);
- *transparence des informations*: article 12, paragraphe 1;
- *exercice des droits:* article 12, paragraphe 2;
- *consentement de l'enfant:* article 8
- *consentement éclairé*: article *7*, lu en combinaison avec l'article 4, point 11;

[83] Cette interface est étroitement liée à un type d'interface trompeuse appelé «*jouer avec les émotions*» évoqué, notamment, dans des rapports d'organisations intergouvernementales, tels que les suivants: Commission européenne, direction générale de la justice et des consommateurs, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., e. a., *Behavioural study on unfair commercial practices in the digital environment*: *dark patterns and manipulative personalisation: final report* (Enquête comportementale sur les pratiques commerciales déloyales dans l'environnement numérique: interfaces trompeuses et personnalisation par manipulation: rapport final), Office des publications de l'Union européenne, 2022, https://data.europa.eu/doi/10.2838/859030; et OCDE, «Dark commercial patterns», *Documents de travail de l'OCDE sur l'économie numérique*, nº 336, Éditions OCDE, Paris, https://doi.org/10.1787/44f5e846-en

Exemples: CU n° 1, exemples 4, 5 et 6; CU n° 5, exemple 52.

4.3.2 Caché au grand jour

Utiliser, pour les informations ou les outils de contrôle de la protection des données, une technique ou un style visuel qui pousse l'utilisateur vers des options moins restrictives et donc plus intrusives.

Dispositions concernées du RGPD:

- *principe de loyauté*: article 5, paragraphe 1, point a);
- *consentement donné librement:* article 7, lu en combinaison avec l'article 4, point 11;
- *informations claires*: article 12, paragraphe 1;
- *exercice des droits:* article 12, paragraphe 2;

Exemples: CU n° 1, exemple 8, CU n° 3a, exemple 34 (illustration); CU n° 3b, exemple 40 (illustration); CU n° 4, exemple 48.

4.4 Obstruction[84]

Entraver ou bloquer l'utilisateur dans son processus de recherche d'informations ou de gestion des données en rendant l'action difficile ou impossible à exécuter.

4.4.1 Impasse

Alors que l'utilisateur cherche des informations ou un outil de contrôle, il ne les trouve pas, car le lien de redirection ne fonctionne pas ou aucun lien ne leur est proposé. L'utilisateur est dans l'incapacité d'exécuter cette tâche.

Dispositions concernées du RGPD:

- *informations aisément accessibles*: article 12, paragraphe 1;
- *exercice des droits*: article 12, paragraphe 2;
- *protection des données dès la conception et protection des données par défaut*: article 25, paragraphe 1.

Exemples: CU n° 1, exemples 10 et 11; CU n° 2a, exemple 18; CU n° 3a, exemples 30 et 31; CU n° 4, exemple 43.

[84] Cette catégorie est étroitement liée à la stratégie appelée «*Obstruction*» définie et décrite dans la publication suivante: Gray Colin M., Kou Yubo, Battles Bryan, Hoggatt Joseph et Toombs Austin L., «The Dark (Patterns) Side of UX Design» [le côté (design) trompeur de la conception de l'expérience utilisateur], dans les actes de la conférence de 2018 sur les facteurs humains dans les systèmes informatiques (Montréal QC, Canada) (CHI' 18). 2018, ACM, New York, NY, États-Unis, article 534, 14 pages. https://doi.org/10.1145/3173574.3174108

4.4.2 Processus plus long que nécessaire

Lorsque l'utilisateur tente d'activer un outil de contrôle de la protection des données, le parcours utilisateur est conçu de telle manière qu'il est obligé d'exécuter plus d'actions que nécessaire pour activer des options intrusives relatives aux données. Cela risque de le dissuader d'activer un tel outil.

Dispositions concernées du RGPD:

- *informations aisément accessibles*: article 12, paragraphe 1;
- *exercice des droits*: article 12, paragraphe 2;
- *droit d'opposition*: article 21, paragraphe 1;
- *retrait du consentement:* article 7, paragraphe 3;
- *protection des données dès la conception (et protection des données par défaut*): article 25, paragraphe 1.

Exemples: CU n° 1, exemple 7; CU n° 3a, exemple 32; CU n° 4, exemple 50; CU n° 5, exemples 57 (illustration) et 58.

4.4.3 Action trompeuse

Un décalage entre les informations et les actions mises à la disposition de l'utilisateur l'incite à faire quelque chose qu'il n'a pas l'intention de faire. Il est probable que la différence entre les attentes de l'utilisateur et le résultat obtenu le dissuade d'aller plus loin.

Dispositions concernées du RGPD:

- *transparence des informations*: article 12, paragraphe 1;
- *loyauté du traitement*: article 5, paragraphe 1, point a).
- *consentement éclairé*: article 7, paragraphe 2, lu en combinaison avec l'article 4, point 11.

Exemples: CU n° 1, exemple 3; CU n° 3a, exemple 28.

4.5 Inconstance

Face à l'instabilité et à l'incohérence de la conception de l'interface, l'utilisateur a du mal à déterminer la nature du traitement, à faire un choix approprié en ce qui concerne ses données, et à trouver les différents outils de contrôle.

4.5.1 Manque de hiérarchie

On observe un manque de hiérarchie dans les informations relatives à la protection des données, de sorte qu'elles apparaissent à plusieurs reprises et sont présentées de plusieurs manières. L'utilisateur risque d'être désorienté face à cette redondance et de ne pas pouvoir comprendre pleinement comment ses données sont traitées et comment exercer un contrôle sur celles-ci.

Dispositions concernées du RGPD:

- *informations aisément accessibles*: article 12, paragraphe 1;

- *exercice des droits: article 12, paragraphe 2.*

Exemples: CU n° 2a, exemples 13 et 14.

4.5.2 Décontextualisation

Une information ou un outil de contrôle en lien avec la protection des données se trouve sur une page hors contexte. Il est peu probable que l'utilisateur trouve cette information ou cet outil de contrôle car il ne les rechercherait pas intuitivement sur cette page spécifique.

Dispositions concernées du RGPD:

- *informations aisément accessibles*: article 12, paragraphe 1;
- *transparence des informations*: article 12, paragraphe 1;
- *exercice des droits: article 12, paragraphe 2.*

Exemples: CU n° 3b, exemples 41 et 42; CU n° 5, exemples 59 et 60.

4.5.3 Interface incohérente

Une interface n'est pas cohérente dans différents contextes (par exemple, un menu relatif à la protection des données n'affiche pas les mêmes éléments sur un appareil mobile et sur la version de bureau) ou par rapport aux attentes de l'utilisateur (par exemple, deux options dont l'emplacement a été interverti). Ces différences peuvent empêcher l'utilisateur de trouver l'outil de contrôle ou l'information souhaité, ou l'amener à interagir avec un élément de l'interface par habitude, même si cette interaction le conduit à faire un choix contre son gré en matière de protection des données.

Dispositions concernées du RGPD:

- *informations aisément accessibles*: article 12, paragraphe 1;
- *exercice des droits: article 12, paragraphe 2.*

Exemples: CU n° 3b, exemple 39; CU n° 4, exemple 50.

4.5.4 Discontinuité linguistique

Les informations relatives à la protection des données ne sont pas fournies dans la ou les langues officielles du pays où réside l'utilisateur, contrairement au service. Si l'utilisateur ne maîtrise pas la langue dans laquelle les informations relatives à la protection des données sont fournies, il ne pourra pas les lire aisément et ne saura donc probablement pas comment ses données sont traitées.

Dispositions concernées du RGPD:

- *loyauté du traitement*: article 5, paragraphe 1, point a);
- *informations compréhensibles:* article 12, paragraphe 1, articles 13 et 14;

- *informations fournies dans des termes clairs et simples*: article 12, paragraphe 1, articles 13 et 14.

Exemples: CU n° 2a, exemple 16; CU n° 3a, exemples 26 (illustration) et 27; CU n° 4, exemple 44.

4.6 Brouillage

L'interface est conçue de manière à dissimuler des informations ou des outils de contrôle de la protection des données, ou à laisser l'utilisateur dans l'incertitude quant à la façon dont ses données sont traitées et au type de contrôle qu'il pourrait avoir sur ce traitement.

4.6.1 Informations contradictoires

Fournir à l'utilisateur des éléments d'information qui se contredisent d'une manière ou d'une autre. L'utilisateur risque de ne pas savoir ce qu'il doit faire et de ne pas connaître les conséquences de ses actions, ce qui l'incitera probablement à ne rien faire et à conserver les paramètres par défaut.

Dispositions concernées du RGPD:

- *loyauté du traitement*: article 5, paragraphe 1, point a);
- *transparence des informations*: article 12, paragraphe 1;
- *consentement éclairé*: article 7, paragraphe 2, lu en combinaison avec l'article 4, point 11.

Exemples: CU n° 2a, exemple 12; CU n° 2c, exemple 20; CU n° 3b, exemple 36.

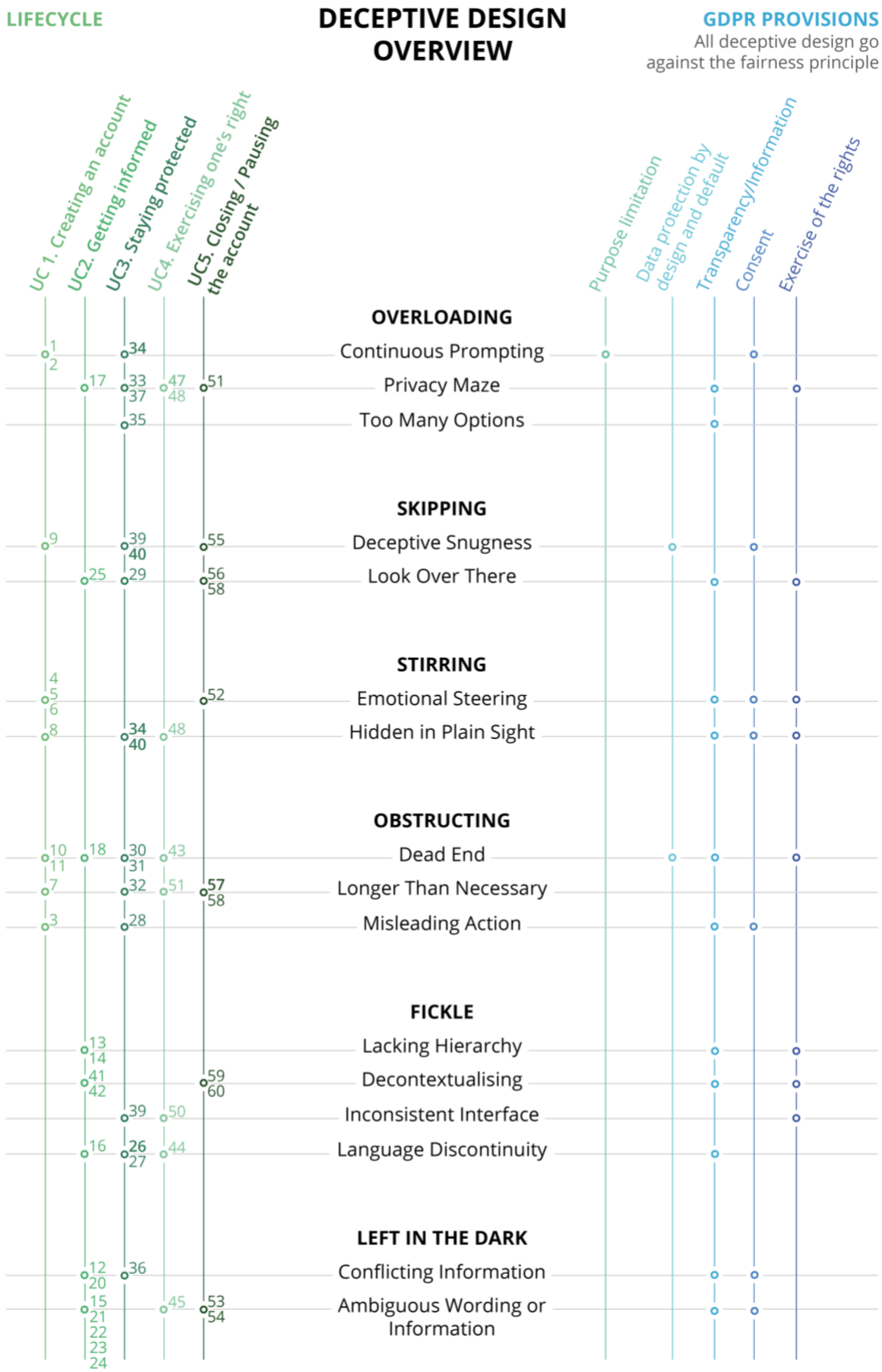
4.6.2 Formulations ou informations ambiguës

Utiliser des termes ambigus et vagues dans les informations fournies à l'utilisateur. Celui-ci risque de ne pas savoir comment ses données seront traitées ou comment exercer un contrôle sur ses données à caractère personnel.

Dispositions concernées du RGPD:

- *loyauté du traitement*: article 5, paragraphe 1, point a);
- *transparence des informations*: article 12, paragraphe 1;
- *informations fournies dans des termes clairs et simples*: article 12, paragraphe 1;
- *consentement éclairé*: article 7, paragraphe 2, lu en combinaison avec l'article 4, point 11;
- *informations incomplètes:* article 13;
- *dispositions spécifiques selon le cas d'utilisation. Par exemple, l'article 34 pour le CU n° 2c.*

Exemples: CU n° 2a, exemple 15; CU n° 2c, exemples 21, 22, 23 et 24; CU n° 4, exemple 45; CU n° 5, exemples 53 et 54.


LIFECYCLE
DECEPTIVE DESIGN OVERVIEW
GDPR PROVISIONS
All deceptive design go against the fairness principle
UC 1. Creating an account
UC2. Getting informed
UC3. Staying protected
UC4. Exercising one's right
UC5. Closing / Pausing the account
Purpose limitation
Data protection by design and default
Transparency/Information
Consent
Exercise of the rights
OVERLOADING
Continuous Prompting
Privacy Maze
Too Many Options
SKIPPING
Deceptive Snugness
Look Over There
STIRRING
Emotional Steering
Hidden in Plain Sight
OBSTRUCTING
Dead End
Longer Than Necessary
Misleading Action
FICKLE
Lacking Hierarchy
Decontextualising
Inconsistent Interface
Language Discontinuity
LEFT IN THE DARK
Conflicting Information
Ambiguous Wording or Information

5 ANNEXE II: BONNES PRATIQUES

La liste suivante donne une vue d'ensemble des bonnes pratiques décrites dans les présentes lignes directrices, à la fin de chaque cas d'utilisation. Ces bonnes pratiques peuvent être utilisées pour concevoir des interfaces utilisateur qui facilitent la mise en œuvre effective du RGPD. Elles peuvent constituer une première étape vers la création d'une solution uniformisée permettant à l'utilisateur de contrôler efficacement ses données et d'exercer ses droits.

Raccourcis: des liens vers des informations, des actions ou des paramètres pouvant aider concrètement l'utilisateur à gérer ses données et ses paramètres de protection des données devraient être proposés partout où il est confronté à des informations ou à des expériences connexes (*par exemple, des liens redirigeant vers les parties pertinentes de la politique de confidentialité*; *par exemple, dans la politique de confidentialité, prévoir, pour chaque information sur la protection des données, des liens qui redirigent directement vers les pages relatives à la protection des données sur la plateforme de médias sociaux; fournir à l'utilisateur un lien leur permettant de réinitialiser son mot de passe; lorsque l'utilisateur est informé d'un aspect du traitement, il est invité à définir ses préférences en matière de données sur la page correspondante des paramètres/du tableau de bord; fournir un lien vers la suppression du compte dans le compte d'utilisateur).*

Options groupées: combiner des options ayant la même finalité de traitement, afin que l'utilisateur puisse les modifier plus facilement, tout en lui laissant la possibilité de procéder à des changements plus précis. Si les plateformes de médias sociaux présentent des options groupées, celles-ci ne devraient pas contenir d'éléments inattendus ou sans lien entre eux (par exemple, des éléments ayant des finalités différentes). Si le traitement nécessite un consentement, les options groupées doivent être conformes aux lignes directrices de l'EDPB sur le consentement, en particulier à leurs points 42 à 44.

Coordonnées: l'adresse de contact de la société à laquelle l'utilisateur peut envoyer des demandes concernant la protection des données devrait être clairement indiquée dans la politique de confidentialité. Elle devrait figurer dans une section où l'utilisateur peut s'attendre à la trouver, par exemple une section concernant l'identité du responsable du traitement des données, une section relative aux droits ou une section de contact.

Contacter l'autorité de contrôle: indiquer l'identité précise de l'autorité de contrôle et insérer un lien vers son site internet ou vers la page internet consacrée à l'introduction d'une réclamation. Ces informations devraient figurer dans une section où l'utilisateur peut s'attendre à les trouver, par exemple une section relative aux droits.

Aperçu de la politique de confidentialité: au début ou en haut de la politique de confidentialité, insérer une table des matières (dépliable) avec des titres et des sous-titres indiquant les différents passages de la déclaration de confidentialité. Les noms des différents passages indiquent clairement à l'utilisateur le contenu exact et lui permettent de repérer et d'atteindre rapidement la section qu'il recherche.

Détection des changements et comparaison: lorsque des modifications sont apportées à la déclaration de confidentialité, donner accès aux versions antérieures, en indiquant la date de leur publication et en mettant en évidence les changements effectués.

Formulation cohérente: il convient d'utiliser une formulation et une définition identiques pour le même dispositif de protection des données sur l'ensemble du site internet. La formulation utilisée dans la politique de confidentialité devrait être identique à celle utilisée sur le reste de la plateforme.

Fournir des définitions: en cas d'utilisation de mots ou de jargon non familiers ou techniques, fournir une définition en des termes simples aidera l'utilisateur à comprendre les informations qui lui sont communiquées. La définition peut être donnée directement dans le texte, lorsque l'utilisateur passe sur le mot, ou figurer dans un glossaire.

Mettre en évidence les éléments relatifs à la protection des données: rendre visuellement frappants les éléments ou actions liés à la protection des données dans une interface qui ne concerne pas directement ce sujet. Par exemple, lors de l'affichage d'un message public sur la plateforme, les outils permettant de contrôler l'association de la géolocalisation devraient être directement disponibles et clairement visibles.

Intégration de la protection des données: aussitôt après la création d'un compte, inclure des points relatifs à la protection des données dans l'expérience d'accueil du fournisseur de médias sociaux pour que l'utilisateur découvre et définisse ses préférences sans difficulté. Par exemple, l'inviter à définir ses préférences en matière de protection des données après avoir ajouté son premier ami ou partagé son premier post.

Utilisation d'exemples: outre les informations obligatoires indiquant de façon claire et précise la finalité du traitement, des exemples peuvent être utilisés pour illustrer un traitement de données spécifique et le rendre ainsi plus concret pour l'utilisateur.

Navigation «collée»: lors de la consultation d'une page relative à la protection des données, la table des matières peut rester affichée en permanence sur l'écran, permettant ainsi à l'utilisateur de toujours se situer sur la page et de naviguer rapidement dans le contenu grâce à des liens d'ancrage.

Retour au début de la page: insérer un bouton de retour au début de la page en bas de la page ou un élément fixe au bas de la fenêtre afin de faciliter la navigation de l'utilisateur sur une page.

Notifications: les notifications peuvent être utilisées pour sensibiliser l'utilisateur aux aspects, aux changements ou aux risques liés au traitement des données à caractère personnel (*par exemple, en cas de violation de données*). Ces notifications peuvent être mises en œuvre de plusieurs manières, par exemple par des messages dans la boîte de messagerie, des fenêtres «pop-in», des bandeaux fixes en haut de la page internet, etc.

Expliquer les conséquences: lorsque l'utilisateur souhaite activer ou désactiver un outil de contrôle de la protection des données, ou donner ou retirer son consentement, l'informer de manière neutre des conséquences d'une telle action.

Cohérence entre les différents appareils: lorsque la plateforme de médias sociaux est accessible à partir de différents appareils (par exemple, ordinateur, smartphones, etc.), les informations et les paramètres relatifs à la protection des données devraient se trouver aux mêmes endroits dans les différentes versions et être accessibles par le même biais et les mêmes éléments d'interface (menu, icônes, etc.).

Répertoire de la protection des données: pour permettre à l'utilisateur de naviguer facilement dans les différentes sections du menu, lui présenter une page aisément accessible à partir de laquelle il aura accès à toutes les actions et informations relatives à la protection des données. Cette page peut se

trouver dans le menu de navigation principal du fournisseur de médias sociaux, dans le compte d'utilisateur, dans la politique de confidentialité, etc.

Informations contextuelles: en plus d'une politique de confidentialité exhaustive, apporter de brèves informations au moment le plus opportun pour que l'utilisateur dispose en permanence d'informations spécifiques sur la manière dont ses données sont traitées.

URL explicite: les pages concernant les informations ou les paramètres relatifs à la protection des données doivent avoir une adresse web qui reflète clairement leur contenu. Par exemple, une page centralisant le contrôle de la protection des données pourrait avoir une URL telle que [réseau-social.com]/paramètres-données.

Formulaire d'exercice des droits: pour permettre à l'utilisateur d'exercer facilement les droits que lui confère le RGPD, fournir un formulaire spécifique qui l'aide à comprendre ses droits et lui indique la marche à suivre pour effectuer ces types de demandes.