Comments on the **EDPB DPIA Template**

The DPIA Template is a useful document, and I thank you for your work on this.

It is a document useful for controllers, but also – though indirectly – for citizens as data subjects, who, thanks to this Template, would be able to get increased awareness about the requirements of the processing of personal data subject to DPIA.

However, I think we need **to integrate the Template with a field on Lawfulness, data protection principle established under Article 5(1)(a) of the GDPR**.

More precisely, *before section 2.1.a of the Template*, a section on Article 5(1)(a) GDPR, according to which "personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')" should be added. I provide a sub-table below in line with the Table's graphics.

2.1 Lawfulness, fairness and transparency of the processing
2.1.a Lawfulness

Overall context of the data processing, including *which data* and *how* they are processed (including for instance if access to terminal devices as defined under the ePrivacy Directive) and the *use-case, purpose* of the data processing	**Mapping of applicable laws** determining which personal data or processing (e.g. profiling) is excluded or subject to specific conditions by law; assessment of **compliance with fundamental rights at stake**	**Justification**
	e.g. remote surveillance of workers if for safety and accompanied by authorisation data processing from IoT or IoB risk assessment for health insurance (eligibility and pricing) work management of platform workers dignity at workplace	e.g. authorisation for remote surveillance of workers obtained by competent labour inspectorate; ePrivacy consent obtained to access to data from terminal devices; processing of genetic data excluded in accordance with insurance law; data related to emotional status of worker excluded in accordance with Platform Work Directive, *etc.*

As recent example, of assessment of lawfulness (in Italia, "liceità del trattamento"[1]) in the light of the applicable legal framework concerning workplaces and of the principle of dignity of workers, see Decision by the Italian DPA of 14 May 2026 on 'sentiment detection' at workplace.[2]

A. Why is this addition in line with the data protection legal framework?

As highlighted by the UK DPA (ICO)[3],:
'The controller must:

- identify valid grounds under the UK GDPR (known as a 'lawful basis') for collecting and using personal data;
- ensure that it does not do anything with the data in breach of any other laws;
- use personal data in a way that is fair. This means the controller must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned;
- be clear, open and honest with people from the start about how it will use their personal data.

---

[1] "Il principio di liceità del trattamento dei dati personali stabilisce che i dati personali devono essere trattati **lealmente e lecitamente**, quindi nel rispetto delle leggi, anche di quelle che regolano settori specifici." https://protezionedatipersonali.it/liceita-del-trattamento

[2] **"4. Il quadro normativo in materia di protezione dei dati personali e tutela della dignità dei lavoratori.**
"[..] occorre ricordare che, in generale, con riferimento ai trattamenti effettuati nel contesto lavorativo, i datori di lavoro devono, tra l'altro, rispettare le norme nazionali, che "includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati in particolare per quanto riguarda la trasparenza del trattamento […] e i sistemi di monitoraggio sul posto di lavoro" (artt. 6, par. 2, e 88, par. 2, del Regolamento).
Sul punto, si fa in particolare presente che l'art. 113 del Codice ("Raccolta dati e pertinenza"), confermando l'impianto anteriore alle modifiche apportate dal d.lgs. 10 agosto 2018, n. 101, fa espresso rinvio alle disposizioni nazionali di settore che tutelano la dignità delle persone sul luogo di lavoro e che vietano al datore di lavoro di raccogliere dati non pertinenti rispetto all'attività lavorativa (artt. 8 della l. 20 maggio 1970, n. 300, e 10 del d.lgs. n. 297/2003, la cui violazione è peraltro penalmente sanzionata, cfr. art. 171 del Codice), la cui osservanza, per effetto di tale rinvio e tenuto conto dell'art. 88, par. 2, del Regolamento, costituisce una condizione di liceità del trattamento.
Nella cornice normativa sopra delineata, le informazioni riguardanti la sfera emotiva dei dipendenti, dunque il relativo stato di benessere o stress psicologico, costituiscono informazioni riconducibili all'ambito di applicazione dell'art. 113 del Codice, la cui conoscibilità è dunque preclusa al datore di lavoro.
Analogamente, il perseguimento della dichiarata finalità "di medicina preventiva, diagnosi e assistenza" (v. informativa resa agli interessati) deve ritenersi radicalmente precluso al datore di lavoro, non solo in ragione delle richiamate disposizioni che vietano l'acquisizione di informazioni non pertinenti rispetto all'attività lavorativa e del tradizionale divieto incombente sul datori di lavoro di assumere in via autonoma iniziative di accertamento sanitario sui dipendenti (v. art. 5 della l. 20 maggio 1970, n. 300), ma anche tenuto conto della stessa circostanza che la predetta finalità è caratterizzata da una dimensione di natura pubblicistica che, nel quadro della disciplina sulla tutela della salute e della sicurezza sul luogo di lavoro, costituisce nel contesto lavorativo espressione di una competenza propria del solo medico competente (v. d. lgs. n. 81/2008; v. anche, più in generale, art. 5 della l. 20 maggio 1970, n. 300).
Tanto, anche nel rispetto di quel tradizionale riparto di competenze e separazione di ruoli tra il medico competente e il datore di lavoro, in cui risiede il principale elemento di garanzia delle norme che, nel disciplinarne compiti e funzioni, prevedono limiti, condizioni e presupposti per il trattamento dei dati nell'ambito di tale specifico contesto (cfr., per analoghe considerazioni, Documento di indirizzo del 14 maggio 2021 recante "Il ruolo del "medico competente" in materia di sicurezza sul luogo di lavoro, anche con riferimento al contesto emergenziale", doc. web n. 958536)."

[3] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/lawfulness-fairness-and-transparency/

Checklist

Lawfulness

☐ We have identified an appropriate lawful basis (or bases) for our processing.

☐ If we are processing special category data or criminal offence data, we have identified a condition for processing this type of data.

☐ We don't do anything generally unlawful with personal data.

Fairness

☐ We have considered how the processing may affect the individuals concerned and can justify any adverse impact.

☐ We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified.

☐ We do not deceive or mislead people when we collect their personal data.

Transparency

☐ We are open and honest, and comply with the transparency obligations of the right to be informed.'

∘

In a similar way, a well-known commentary to the GDPR[4] specifies that "*the requirement that data processing must be lawful essentially means that it respects all applicable legal requirements (for example the obligation of professional secrecy if applicable)*"[5]. Moreover, "*the principle of lawful processing is also to be understood by reference to conditions for lawful limitations of the right to data protection or of the right to respect for private life in light of Article 52 of the Charter if Fundamental Rights of the European Union ('CFR') and of Article 8(2) ECHR*."[6]

[4] "The EU General Data Protection Regulation (GDPR), A Commentary", Oxford University Press, 2020.
See also Eleni Kosta & Franziska Boehm (eds), "The Law Enforcement Directive: A Commentary", Oxford University Press; Article 8. Lawfulness of processing: "The principle of 'lawful processing' together with 'fair processing' is one of the data protection principles under Article 4 LED and its corresponding Article 5 GDPR. In fact, the principle of 'lawful and fair processing' is seen as the 'primary' principle that 'embraces and generates' all the other data processing principles."

[5] *Ibidem*, at page 314.

[6] *Ibidem*, at page 314.

In the same way the *transparency* principle is an overarching data protection principle that is specified under but not limited to the articles in Section 1 and 2 of Chapter III of the GDPR[7], the *lawfulness* principle, also an overarching principle, is specified under but not limited to Article 6 laying down the legal basis for the processing of personal data[8].

Again, as specified by ICO,
Lawfulness is not all about Article 6 GDPR legal basis, or Article 9 conditions.
"Lawfulness also means that you don't do anything with the personal data which is unlawful in a more general sense. This includes statute and common law obligations, whether criminal or civil. If processing involves committing a criminal offence, it will obviously be unlawful. However, processing may also be unlawful if it results in:
- a breach of a duty of confidence;
- your organisation exceeding its legal powers or exercising those powers improperly;
- an infringement of copyright;
- a breach of an enforceable contractual agreement;
- a breach of industry-specific legislation or regulations; or

---

[7] https://www.edpb.europa.eu/system/files/2023-01/edpb_bindingdecision_202205_ie_sa_whatsapp_en.pdf
"145. The EDPB underlines that the principles of fairness, lawfulness and transparency, all three enshrined in Article 5(1)(a) GDPR, are three distinct but intrinsically linked and interdependent principles that every controller should respect when processing personal data. The link between these principles is evident from a number of GDPR provisions: recitals 39 and 42, Article 6(2) and Article 6(3)(b) GDPR refer to lawful and fair processing, while recitals 60 and 71 GDPR, as well as Article 13(2), Article 14(2) and Article 40(2)(a) GDPR refer to fair and transparent processing.
146. The IT SA states that "the infringement of Article 5(1)(a) GDPR should be found by the LSA in the case at hand by having also regard to the more general fairness principle, which entails separate requirements from those relating specifically to transparency."
See also paragraphs 99, 101, 309, 318.

[8] See for example CJEU 'Mousse' case, C-394/23, establishing a 'cascade' from lawfulness as principle to GDPR legal basis, including consent, to the rules on consent (from the broader provision to the more specific ones):
"a. Data protection principles
21. (..) the objective pursued by the GDPR, as is set out in Article 1 thereof and in recitals 1 and 10 thereof, consists, inter alia, in ensuring a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data, as enshrined in Article 8(1) of the Charter and Article 16(1) TFEU
(..).
22. In accordance with that objective, any processing of personal data must, inter alia, comply with the principles relating to the processing of such data set out in Article 5 of that regulation and satisfy the lawfulness conditions listed in Article 6 of that regulation (..).
23. Article 5(1)(a) of the GDPR provides that personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
24. Under Article 5(1)(c) of that regulation, which enshrines the principle of data minimisation, those data must also be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. That principle gives expression to the principle of proportionality (..)
°
b. Legal basis for the processing of personal data
25. As regards the conditions for lawful processing, as the Court has held, the first subparagraph of Article 6(1) of the GDPR sets out an exhaustive and restrictive list of the cases in which processing of personal data can be regarded as lawful. Thus, in order to be capable of being regarded as such, processing must fall within one of the cases provided for in that provision (..).
°
c. Consent
26. Under point (a) of the first subparagraph of Article 6(1) of the GDPR, the processing of personal data is lawful if and to the extent that the data subject has given consent for one or more specific purposes. In the absence of such consent, or where that consent is not freely given, specific, informed and unambiguous, within the meaning of Article 4(11) of the GDPR, such processing is nevertheless justified where it meets one of the requirements of necessity mentioned in points (b) to (f) of the first subparagraph of Article 6(1)"

- a breach of the Human Rights Act 1998.
These are just examples, and this list is not exhaustive. You may need to take your own legal advice on other relevant legal requirements."[9]

B. Why is this addition needed to protect citizens, persons concerned, notably at the 'age of AI'?

From a practical point of view, referring to Lawfulness in the Template is important because it would recall controller to **first check key aspects of compliance** of the data processing, which are:

- **compliance with sectorial laws** (e.g. conditions and limits on remote surveillance of workers having regard to employment law; data that cannot be processed even if the data subject consents to the processing, under insurance law or consumer credit law; compliance with intellectual property law; compliance with DSA in case of online platforms subject to this EU law, *etc*.);

- for data processing which already appear as problematic due to fundamental rights' concerns: checking **compliance with fundamental rights as provided by the Charter** (e.g. human dignity; non-discrimination).

Including lawfulness as overarching principle under the GDPR would also clarify that **the data subjects' exercise of their data protection rights** (for instance, the right of access) can indeed aim at checking the **lawfulness of the processing** of their data and, in doing so, be assured about **compliance of the data processing with sectorial law (employment or consumer credit or insurance law) and with human rights' law and principles**.

Why is lawfulness of data processing so important for AI Act implementation whenever personal data are processed, notably when the AI model or system is deployed?

Because the processing of personal data entailed by certain high-risk AI systems is not (or is likely not to be) compatible with fundamental rights and/or with sectorial laws. It is indeed such compatibility that should first be checked assessing **lawfulness**.

Examples (most of which in the recent draft Commission's Guidelines on the classification of high-risk AI systems):
- a consular authority uses an AI as lie detector that analyses an applicant's voice patterns and verbal responses and pupillometry during visa interviews conducted by consular officers;
- ranking of migrants as risks on the basis of screening of their online activities (mobile phones' data extraction);
- remote surveillance on workers in violation of Member State legislation (e.g. in Italy, Statuto dei lavoratori);
- AI to influence the outcome of a referendum;
- gen-AI used for selection/ranking of candidates by a public admin (who needs to act on the basis of pre-determined criteria to justify its decisions); etc.

[9] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/lawfulness-fairness-and-transparency/#lawfulness

C. A key distinction: compliance which is 'not negotiable' *versus* assessment of risks to be mitigated

The addition of a Section dedicated to Article 5(1)(a) Lawfulness at page 9 of the Template, under Chapter 2 of the Template (separate from and before Chapter 4 of the Template, on risk assessment and management), is also helpful because it signals to the controller the distinction between:

« *La démarche de conformité mise en œuvre en menant un PIA repose sur deux piliers:*
1. les principes et droits fondamentaux « non négociables », qui sont fixés par la loi et doivent être respectés, quels que soient la nature, la gravité et la vraisemblance des risques encourus;

2. la gestion des risques sur la vie privée, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données. »[10]

Translated in EN:
"*The approach to compliance implemented by conducting a DPIA is based on two pillars:*

1. *"non-negotiable" fundamental principles and rights (I add, including rights or limitation on data processing, so-called 'personal data boundaries, stemming from applicable sectorial laws such as labour law etc), which are established by law and must be respected regardless of the nature, severity, and likelihood of the risks incurred;*
2. *privacy risk management, which determines the appropriate technical and organizational measures to protect data*."

Regrettably, the 'AI narrative' built around the use of AI models and systems often ignores the non-negotiability of principles and rights from primary or secondary applicable Union or national legislation and shifts to the second 'pillar', as risk-management, the (non-negotiable) compliance with fundamental rights and principles[11].

This is **not correct under the legal viewpoint** (it ignores the assumption of overall consistency of the legal order) and of course **lowers the protection** for persons concerned.

It is therefore more important than ever to highlight – also in this Template as checklist – the **autonomy and key relevance of the Lawfulness data protection principle**, to be put at front and centre of controller's compliance attention, as **overarching principle** meaning that the data processing must be in compliance with all applicable legal requirements stemming from EU and Member State law.

---

[10] https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-fr-methode.pdf at page 3.

[11] See Martin Ebers, "*Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act*", European Journal of Risk Regulation (2025), 16, 684–703, at page 690: "the EU's decision to protect human rights in the AI Act primarily through a risk-based approach, rather than of a rights-based approach, is generally ill-suited. Most importantly, such an approach neglects the minimum and non-negotiable nature of human rights. Instead, the AI Act, with its risk-based approach and its fundamental rights impact assessment, implies that fundamental rights violations can be quantified and measured in degrees. This is, however, not the case. As Yeung & Bygrave point out, while it is possible to speak of different levels of culpability, scale, and magnitude when talking about fundamental rights, "these variations do not imply that fundamental rights violations can be, without problems, ranked on a sliding scale from trivial to serious." Instead, fundamental rights follow a binary logic in that an activity is either legal or illegal."

Example:
lawfulness as respect of human dignity (having regard to particularly invasive the processing of sensitive data processing such as of biometric data and special categories of personal data).
Before considering (if) consent of the person who would be affected by the use of invasive technology, need to assess Lawfulness:
"Lawfulness of neuro-data processing.
Once its purpose has been specified, and provided that the processing of neuro-data is compliant with fundamental rights, and in particular with the principle of necessity and proportionality of any interference with the fundamental right to privacy and to the protection of personal data, neuro-data processing can be lawful only if and to the extent that, among other conditions, the appropriate legal basis is relied upon by the controller. These legal bases include: [..]"
International Working Group on Data Protection in Technology (IWGDPT), Working Paper on "Emerging Neuro-technologies and data protection", 15 May 2025.