1 Who is UNIDPO

UNIDPO (Unione Nazionale Italiana Data Protection Officer, i.e., *Italian National Union of Data Protection Officers*) is a "no profit" association founded on 26th May 2018 by over seventy professionals, lawyers and engineers, united by an interest in the matter of privacy, personal data protection and IT security.

The idea of UNIDPO was born during the first "Corso di alta formazione sulla protezione dei dati personali per la formazione del Responsabile della Protezione dei Dati (Data Protection Officer – DPO)" (*"Advanced training course on personal data protection for the training of the (Data Protection Officer - DPO)"*), jointly organized by the National Forensic Council (CNF) and the National Council of Engineers (CNI), under the patronage of the Italian Data Protection Authority, on a project of the Italian Foundation for Forensic Innovation (FIIF).

The peculiarity of the course, involving two quite inhomogeneous professions, both in terms of forma mentis and scientific training, made it possible to highlight the fruitfulness of a multidisciplinary approach to the subject of data protection, and to make conscious the founders of UNIDPO that skills and experiences necessary to professionally deal with privacy and data protection can only mature through the synergy between different "visions".

Hence, the idea that inspired the foundation of UNIDPO was to create a network of professionals with different and complementary experiences and skills, to be mutually transferred, possibly also providing team services to customers.

Therefore, even if founded by lawyers and engineers, UNIDPO welcomes among its members everyone dealing professionally with privacy, personal data protection and IT security, provided they are highly qualified to play the role of DPO or data protection consultant by means of specific and certified skills.

The general purpose of the association is also to spread the culture of privacy and of personal data protection - helping to raise the level of awareness of individuals about the immense value of personal data – and also to support the training of members, raise awareness of the community on the ethical role and social security of the DPO, spreading the culture of information security and information as well as the protection of individuals' rights and freedoms, on the assumption that technology is at the service of man.

The association currently counts about one hundred members and nurtures the ambitious aspiration to become a group of excellence in training and dissemination - internal and external - on the issues inherent the GDPR.

UNIDPO is a still young Association, but it has clear targets. All of them are underpinned by a common principle: ethics. This is the idea permeating UNIDPO activities in terms of promoting data value awareness and diffusing virtuous and ethical behaviours in data collection and data processing.

1.1 Team for DPbDD Guidelines' analysis

Andrea Praitano (Team Leader of DPbDD UNIDPO's team and Member of Ethics Committee).

Andrea D'Amico (DPbDD UNIDPO's Team Member).

Federico Fogal (DPbDD UNIDPO's Team Member).

Giovanni De Marco (DPbDD UNIDPO's Team Member and Board Member).

Giuseppe Giovanni Zorzino (DPbDD UNIDPO's Team Member).

Mara Parpaglioni (DPbDD UNIDPO's Team Member).

Michelino Chionchio (DPbDD UNIDPO's Team Member and Board Member).

2 Comments on the Guidelines for DPbDD

In this section we share our observations regarding the "*Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*" (hereinafter the "**Guidelines**"). We will provide our comments in three different subsections:

- in the first subsection we will share our general remarks on the Guidelines;
- the second subsection contains comments on specific points or paragraphs of the Guidelines;
- in the third subsection we will submit to the European Data Protection Board ("**EDPB**" or the "**Board**") some examples that, in our opinion, may help clarify the scope of the "data protection privacy by design and default" legal obligation (hereinafter also the "**DPbDD**") set forth in article 25 of the Regulation no. 2016/679/UE ("**GDPR**").

2.1 General comments on the Guidelines

UNIDPO 1. The main content of the Guidelines can be virtually divided into two parts: while the first part analyses article 25 of the GDPR (section # 2 of the Guidelines) the second part (section # 3 of the Guidelines) provides some "real life" examples meant to help any organization in handling the DPbDD requirement. We approve the overall structure of the Guidelines and, especially, believe that the presence of "real life" examples together with an explanatory part is consistent with the goals of the Guidelines and helps in illustrating the DPbDD requirement and the multiple aspects underlying article 25 of the GDPR.

UNIDPO 2. All the above being said regarding the overall structure of the Guidelines, with reference to their content we would have welcome a more in-depth analysis of the DPbDD requirement, narrower definitions of the key concepts set forth by article 25 of the GDPR as well as further and more specific examples regarding the practical applications of such key concepts. Although we understand that the actual content of the Guidelines undergoing public consultation is indeed due to (we may even say: forced by) the broad material scope of the GDPR itself as set forth in article 2 of the GDPR, we find that the Board should refrain from broad definitions (as appear to be some of those contained within the Guidelines) in order to fulfill the task of which EDPB was appointed according to consideration 139 and article

70 (1) (e) of the GDPR. As far as we are concerned, in fact, broad definitions may lead to incoherent application of the GDPR among the Member States, thus ending in a breach of the principles of "equality before the law" and "non-discrimination" set forth in articles 20 and 21 (2) of the Charter of the Fundamental Rights of the E.U.. For the sake of clarity (and warning the reader that we'll explain in greater details our opinion in the following subsection), some of the key concepts that we find broadly defined are those of "state of the art" and "cost of implementation".

UNIDPO 3. In light of the above we encourage the EDPB to provide a more in-depth analysis of article 25 of the GDPR: section # 2 of the draft Guidelines undergoing public consultation, in fact, appears to be more concerned in listing all the aspects that a data controller (and also, to some extent, a data processor) need to check while designing and carrying out a data processing than in giving applicable benchmarks for assessing each of those aspects. A more in-depth analysis together with clear (and, possibly, narrow) definitions of the key concepts contained in article 25 of the GDPR would provide further guidance for complying with the DPbDD requirement as well as help defining a clear-cut border between the obligations set forth in articles 25 and 32 of the GDPR (obligations which appear to overlap one with the other, as we will observe later in details in the following subsection).

UNIDPO 4. The contents of section # 2 in the guideline explain better the principle and explore the different parts included in the article 25. The explanation of the article could help small and medium organization in the interpretation of the article and them are I line with the examples included in the Guideline. We suggest to add complex example that can help big organization in the implementation of the DPbDD.

UNIDPO 5. Accordingly, we also encourage EDPB to furnish in section # 3 of the Guidelines further "real life" examples providing an in-depth guidance on how to comply with the DPbDD, especially by complex organizations such as Banks, Hospitals and Public Administrations.

UNIDPO 6. In our opinion the guideline, in the current draft version, is focalized on SME and it is not applicable or could not give a real support to big or complex organization. Part of the reasons for this opinion are the points UNIDPO 3 and UNIDPO 5. We suggest to expand the examples included in section # 3 in the guideline with examples for complex and big organizations.

UNIDPO 7. Finally, since the Guidelines appear to contain English as well as American words (e.g. the word "minimisation" which sometimes is also written as "minimization"), we would rather have the Board chose between one of the two aforesaid languages and draft the Guidelines consistently with such choice.

2.2 Detailed comments on specific points of the guideline

Section: 2.1.1 Controller's obligation to implement appropriate technical and organizational measures and necessary safeguards into the processing

Paragraph: # 11

UNIDPO 8. The footnote number 4 includes two technical security measures such as hashing and encryption. Said technical security measures are related to pseudonymization. We find inappropriate to consider the hashing as a possible way to implement the pseudonymization of the data set because the hashing is possible only in one direction and

it's not reversible. The use of hashing could be a possible way for the implementation of pseudonymization but in a complex technical implementation. We suggest to add more details for the use of hashing or delete the hashing from the note number 4.

Section: 2.1.3 Elements to be taken into account – "state of art" and "cost of implementation"

Paragraphs: from # 18 from # 22 and # 24

UNIDPO 9. When defining the concept of "*state of the art*" the Guidelines declare that it "*is a dynamic concept that cannot be statically defined at a fixed point in time*" and "*imposes an obligation on controllers, when determining the appropriate technical and organisational measures, to take account of the current progress in technology that is available in the market*": we find advisable to set up a more in-depth (and possibly objective) criterion to (try to) narrow the concept of "*state of the art*", for considering only the "availability on the market" of a specific technology as stated in the Guidelines may lead to many dissimilar approaches since there are significant differences between technologies that (i) are newly launched on the market, or (ii) have reached a "market maturity", or (iii) are widely used amongst the competitors of the data controller, or (iv) are generally used by the public at large.

UNIDPO 10. At paragraph # 24 the Guidelines state that "*Incapacity to bear the costs is no excuse for non-compliance with the GDPR*". Such statement may have critical effects on subjects, such as Public Administrations, that do not have enough resources but, on the other hand, cannot cease a specific processing unless breaching the law. We ask the Board to please clarify and /or deepen the scope and meaning of the aforementioned statement in light of the above.

Paragraph: # 20

UNIDPO 11. As already observed, the paragraph explains that the "state of art" is a dynamic concept that cannot be statically defined at a fixed point in time. Based on our experience the DPbDD is a continual process that identifies and implements a set of security measures at the design stage of a processing and/or of a device (for example by defining the security requirements of the processing as well as by executing security test during the development phase of an electronic device) and continues updating such measures throughout the lifespan of said processing/device. Only the last sentence of the paragraph expresses this concept clearly, although we find that it could be better stated that the DPbDD is a continual activity and the controller has to identify continually or periodically (for example annually) if the identified security measures are effective or it is necessary implement new security measures, also considering the organizational measure, which the paragraph seems to forget.

UNIDPO 12. In the 32nd Conference of Privacy Authorities in 2010 it was recognized that the concept of "Privacy by Design" is an essential component of fundamental privacy protection. The application of DPbDD is not only for new a processing or system/device but also for pre-existing ones and, from 2010, the system and processing have to be designed accordingly to the "Privacy by Design" requirement. We would like the EPDB to explain deeply the impact of the DPbDD principle upon the pre-existing processing and systems/device.

Section: 2.1.3 Elements to be taken into account – "state of art"

Paragraph: # 22

UNIDPO 13. The paragraph indicates that there are standards and certifications that can support the identification of the state of art for security measures. There are many standards regarding the security measures (e.g. ISO/IEC 27001, ISO/IEC 20000-1, ISO 22301, ISO/IEC 27701, etc.), or, as it seems more appropriate to say, many "couples of standards" since together with a "certification standard" (such as those listed above) usually comes a second standard which states the "code of practice" (e.g. ISO/IEC 27002, ISO/IEC 20000-2, etc.). We observe, however, that together with the standards above mentioned there are also other types of publications coming from renowned organizations (such as ENISA, NIST, etc.) which address the security matter; such documents, which are more often than not as good as the stabdards referred to above, are generally called in different ways ("Special Publication", "Guidelines", etc.). We suggest to include in the sentence not only the generic term "standard" and "certification" but also other terms like "special publication", "code of practice" and "guideline", unless the EDPB effectively means to exclude the latter publications.

Section: 2.1.4 Time aspect – "*At the time of the processing itself*"

Paragraph: # 38

UNIDPO 14. The DPbDD requirement affects the controller(s) as well as the processor(s) involved in the data processing, although pursuant to article 25 of the GDPR the burden of fulfilling the DPbDD is assigned only to the controller. It could be better explained that the controller has to identify the security measures and it must also assign (though a contract) relevant security measures to processors and control the respect of the indications and requirements.

Section: 2.2.1 Required application of data protection by default

Paragraph: # 52

UNIDPO 15. The identification of data retention time is not easy. Data Retention Directive (Directive 2006/24/EC) tried to define some aspect on data retention but it was declared invalid by Court of Justice of the European Union. The data retention is not only a privacy aspect but includes other aspects defined in national laws. We suggest to include an explanation of the keys point to identify the data retention time to help the organization comply with this important and critical aspect.

Section: 5 Enforcement of article 25

Paragraphs: # 84 and # 85

UNIDPO 16. The enforcement of article 25 of the GDPR is partly overlooked by the Guidelines, although, in our point of view, it is a crucial matter that needs to be addressed by EDPB in light of the following observations. Pursuant to article 25 of the GDPR "*(…) the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data*

minimisation, in an effective manner (…)". Accordingly, the Guidelines underline the importance of adopting security measures both technical and organizational which are effective. The security of personal data is also addressed by article 32 of the GDPR, pursuant to which "*(…)the controller and the processor shall implement appropriate technical and organisational measures (..)*". Looking at the abovementioned GDPR articles it may seem that they overlap one with the other. We are not concerned about such overlap, per se: what concerns us, as data professionals, is the possibility that a single omission such as the lack of a security measure may lead the controller to the breach of two different GDPR provisions (if not even three, also considering article 5 GDPR), thus compelling the competent supervisory authority to issue a fine for each breach against said controller, pursuant to articles 83 (4) (a) and/or 83 (5) (a). Said scenario of a single omission fined twice seems to be in breach of the right not to be tried nor punished twice in criminal proceedings for the same criminal offence ("*ne bis in idem*" principle) set forth in article 50 of the Charter of Fundamental Rights of the EU, as interpreted by C.G.E.U. (among the others we may cite C-537/16) according to which article 50 of the Charter prohibits a duplication of proceedings and of penalties which are "criminal in nature" in respect of the same acts and against the same person. Though we know that GDPR doesn't provide any criminal penalty, it must nonetheless be noted that C.G.E.U. expressed the opinion that «*the application of Article 50 of the Charter is not limited to proceedings and penalties which are classified as "criminal" by national law, but extends regardless of such a classification to proceedings and penalties which must be considered to have a criminal nature*» (C-537/16, § 32) on the basis of (i) the nature of the offence and/or of (ii) the degree of severity of the penalty that the person concerned is liable to incur. C.G.E.U. also affirmed that a measure which merely repairs the damage caused by the offence at issue is not "criminal in nature", while an administrative fine which is not only intended to repair the harm caused by the offence, but that also pursues a punitive purpose must be deemed as "criminal in nature". In light of the above, also considering the high fines set forth in articles 83 (4) (a) and 83 (5) (a) (which are "*up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year*") we fear that the scenario depicted above (the omission of a security measure fined twice because considered in breach of articles 25 and 32 GDPR) may contrast with the *ne bis in idem* principle. It must be furthermore noted, that pursuant to article 83 (2) GDPR "*the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32*" is not only a breach per se, but also a factor to be taken into account by the competent supervisory authority when deciding the amount of the administrative fine in each individual case. Therefore, given all the above, it may be the case to analyze in deep the interactions between articles 25 and 32 GDPR and, possibly, define a clear-cut border between the requirements set forth by each article (at least those burdening the controller, since only article 32 seems to affect directly the processor). For instance, it may be reasonable to consider the omitted provision of a security measure at the time of determination and/or review of the means of the processing as in breach of article 25 GDPR, while a breach of article 32 may be the omitted or ineffective implementation of a security measure which has already been considered as necessary as a result of the determination or review of the means of the processing carried out by the controller. In our opinion, however, the draft Guidelines undergoing public consultation lack of said analysis, so therefore we hope that the EDPB will integrate it in the final draft of the Guidelines.

2.3 Suggestion on examples

An organization adopt technical and organizational security measures not only for Data Protection Framework (GDPR, Directive 680/2016, Directive 58/2002, etc.) but also for other laws or standards (for example Directive 2016/1148 on Cybersecurity, PCI-DSS, ISO/IEC 27001:2013, etc.).

Usually an organization has a minimum set of security measures by default (for example the PCs have an antivirus, the network boarder is protected by Firewall, the access is controlled by badge system/reception, etc.). The implementation of the DPbDD in an organization could include a definition of a structured process that evaluate the inputs that request security requirements, evaluate is the standard security measures are sufficient or there are necessary an extra set of security measures.

UNIDPO 17. We suggest to add an example or a list of activities necessary for the implementation of a DPbDD process in an organization.

Milan, 16th January 2020

The President of UNIDPO

Avv. Ugo Carlo Di Nicolo'

DI NICOLO' UGO CARLO
Avvocato
16.01.2020 10:50:36 UTC