STAR II SUPPORT SMALL AND MEDIUM ENTERPRISES ON THE DATA PROTECTION REFORM II

Draft versions of the guidance & handbook

Deliverable **D4.1**

version 1.0

Gábor Kulitsán
Renáta Nagy
Lina Jasmontaite-Zaniewicz
Leanne Cochrane

Budapest – Brussels – Dublin
February 2020

Distribution level: **Public**

LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY STUDIES VRIJE UNIVERSITEIT BRUSSEL

TRILATERAL RESEARCH

A report prepared for the European Commission's Directorate-General for Justice and Consumers (DG JUST).

The STAR II project (*Support small And medium enterprises on the data protection Reform II*; 2018-2020) is co-funded by the European Union under the Rights, Equality and Citizenship Programme 2014-2020 (REC-RDAT-TRAI-AG-2017) under Grant Agreement No. 814775.

Cover image:

Permanent link:

Authors	
Name	**Partner**
Gábor Kulitsán	NAIH
Renáta Nagy	NAIH
Lina Jasmontaite-Zaniewicz	VUB-LSTS
Leanne Cochrane	TRI

Contributors	
Name	**Partner**
Júlia Sziklay	NAIH
Alessandra Calvi	VUB-LSTS
Paul de Hert	VUB-LSTS

Internal Reviewers	
Name	**Partner**
Alessandra Calvi	VUB-LSTS
Lina Jasmontaite-Zaniewicz	VUB-LSTS
Leanne Cochrane	TRI
David Barnard-Wills	TRI

Institutional Members of the STAR Consortium		
Member	**Role**	**Website**
Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)	Project Coordinator	naih.hu
Vrije Universiteit Brussel (VUB) Research Group on Law, Science, Technology and Society (LSTS)	Partner	https://lsts.research.vub.be/
Trilateral Research Ltd. (TRI IE)	Partner	trilateralresearch.com

Table of Contents

1 Background to the STAR II project

The STAR II (SupporT small And medium enterprises on the data protection Reform II) project, running in the partnership of the National Authority for Data Protection and Freedom of Information (NAIH), the Research Group on Law, Science, Technology & Society (LSTS) of the Vrije Universiteit Brussel (VUB), and the Trilateral Research Limited (TRI IE) between 2018 and 2020, has the aim of enhancing compliance with the GDPR by assisting DPAs and SMEs.

There are pressing needs to assist EU data protection authorities (DPAs) in raising awareness among businesses, especially SMEs, on the new EU legal framework for personal data protection, particularly the GDPR. At the same time, SMEs often need external assistance to understand the gravity of the new regulatory regime applicable for the processing of personal data; they need guidance on how to follow their respective Member State national legislation giving full effect to the GDPR; they need to adapt their routine practices; they need to acquire information, solve new or hitherto unnoticed issues and follow trainings on the new legislation; they often need to create and execute an action plan to apply the new framework.

In order to address these needs, the STAR II project will:

1) review the state of the art in DPA awareness-raising activities,
2) analyse SMEs' experience within first months of the functioning of the GDPR,
3) run an awareness raising campaign for SMEs,
4) establish and operate an e-mail hotline (12 months) to respond to SMEs' questions, measuring its performance and the most frequently asked questions,
5) prepare a digital guidance for DPAs on good practices in running an e-mail hotline and raising SME awareness, and
6) draft an innovative, FAQ-based handbook (digital and printed) for SMEs on EU personal data protection law.

These results will be prepared in consultation with stakeholders (especially via validation workshops and the External Advisory Board) and widely disseminated. The outputs will be freely available, openly accessible and copyright-unrestricted, thus easily reusable and adaptable.

2 Summary

This document is comprised from two parts:

Part A - the guidance for DPAs on good practices in raising awareness, especially for SMEs about GDPR issues. The guidance, after situating awareness raising task within the redefined role of DPAs, builds on the experience of NAIH obtained during the timespan of a hotline for SMEs. The guidance provides recommendations on how to set up and run a hotline. It pays special attention to the required infrastructure, resources required, engaged personnel, internal policies, legal implications and ethical considerations.

Part B - an innovative handbook for SMEs on EU data protection law based on the questions SMEs most frequently asked the hotline and the responses given. The responses to be given will help explain to SMEs the basics of data protection law and the GDPR, through illustrations, practical examples, templates and contacts for better understanding and easy utilisation. This handbook will accustom SMEs to the GDPR, and help them ensure that they are GDPR compliant. The handbook will predominantly reflect and build on the issues raised in Activity 3.4. The handbook will also be valuable for DPAs too as it will help them understand which issues are particularly concerning SMEs and where they might wish to be put the emphasis in their own awareness raising activities.

3 Guidance for DPAs on setting up hotlines for SMEs

3.1 The role and powers of DPAs under the GDPR

A significant part of the General Data Protection Regulation EU 2016/679 (GDPR) is devoted to address the role and the daily functioning of Data Protection Authorities (DPAs). The GDPR in Chapter VI on Independent Supervisory Authorities[1], by taking into account the case law of the Court of Justice of EU (CJEU) that has emerged in response to uncertainties concerning the scope of DPAs tasks, responsibilities and their independence, clarifies and, to some extent, redefines responsibilities of DPAs.

The GDPR asserts that the primary responsibility of DPAs concerns the monitoring and consistency of the application of the GDPR 'in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union'.[2] It has been observed that the consistency obligation found in the GDPR does not have an equivalent in the Data Protection Directive 95/46/EC (DPD) that it has repealed.[3] Nonetheless, it can be suggested that this obligation related to the requirement for DPAs to 'cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information' that was set in the DPD.

The legislator has foreseen in Article 57 that to attain the objective of monitoring and consistency of the application of the GDPR, DPAs should undertake 22 tasks that range from enforcers, ombudsmen, auditors, consultants to policy advisors, negotiators and educators.[4] The list leaves no doubt that DPAs responsibilities fall beyond enforcement.[5] Some suggest that overall all these tasks could be seen through different lenses and DPAs could be regarded as a leader, an authoriser, a police officer and a complaint-handler.[6]

The DPA role of the leader – a policy mainstreamer – and the scope of awareness raising duties to the general public, controllers and processors have received little attention. To foster the debate on what do such awareness raising duties include and how their consistency can be ensured among 27 European Union (EU) member states, we put forward this guidance document.

In an attempt to reflect on this long practiced by only recently formalized duty, we will consider the impactions of DPAs as educators.

3.2 DPAs & awareness raising

Dynamics of enforcement powers provided within the scope of the EU data protection framework have shaped awareness raising duties of DPAs. It can be suggested that to compensate for being

[1] When referring to Independent Supervisory Authorities we use the following terms: Data Protection Authorities, DPAs and regulators.
[2] European Union Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ EC (GDPR), Article 51.
[3] Kuner C., Bygrave L., Docksey C., The EU General Data Protection Regulation (GDPR): A Commentary (OUP; 2020), 866.
[4] Cross reference to Bennett, Colin and Charles Raab, The Governance of Privacy: Policy Instruments in Global Perspective, MIT Press, Cambridge MA & London, 2003, p.109–114. in David Barnard-Wills, Cristina Pauner Chulvi and Paul De Hert, 'Data Protection Authority Perspectives on the Impact of Data Protection Reform on Cooperation in the EU' (2016) 32 Computer Law & Security Review 587, 587 <https://linkinghub.elsevier.com/retrieve/pii/S026736491630084X> accessed 3 August 2019.
[5] The list is included at the end of this guidance.
[6] Centre for Information Policy Leadership, 'Regulating for Results Strategies and Priorities for Leadership and Engagement: A Discussion Paper' (2017) p. 7-8.

awarded with limited enforcement powers to impose the so called 'deterrence' style enforcement and significant fines under the Data Protection Directive 95/46/EC, for most of DPAs awareness raising duties have long been part of their enforcement strategies. In view of this, it can be even argued that most of the DPAs followed intuitively the recommendation put forward by Robert Baldwin and Martin Cave in their seminal work on understanding regulation that rules 'have to be employed by enforcers in conjunction with different compliance-seeking strategies – be these prosecutions, administrative sanctions, or processes of persuasion, negotiation, advice, negotiation, education, or promotion'.[7] By means of opinions, guidelines, public engagements and other similar awareness raising activities, the well-intentioned national regulators sought to reach, one the one hand, individuals, whose rights are affected, and, on the other hand, 'controllers' and 'processors', who handle personal data of individuals. However, diverse approaches emerged among DPAs in terms of their tasks and powers as a result of 'history, case law, culture and the internal organization of the Member States'.[8]

The legislators with the adoption of the GDPR sought to reduce such diversity and increase harmonisation among DPAs enforcement practices. It could be argued that formalising awareness raising duties of DPAs could be seen as an attempt to ensure that regulators can enforce the applicable framework 'in a more uniform and effective way' and a way update enforcement practices of DPAs.[9] This being said, it should be added that while awareness raising duties constitute only part of DPAs tasks, they cannot be considered in isolation from other tasks foreseen in the GDPR. Awareness raising has a direct bearing on how the ones who are regulated cope with applicable rules and it also affects enforcement claims brought by individuals.

3.3 Advantages of awareness raising

Awareness raising duties of DPAs should be considered to be instrumental to attain the objective of monitoring and consistency of the application of the GDPR because of several reasons.

First of all, awareness raising activities undertaken by DPAs complement the applicable legislative framework by providing additional explanation of different provisions (e.g., what does the purpose limitation principle entail?). Only the regulation that can be understood in a comprehensive manner, carries the potential to result in the desirable behavior of addressees. In this sense, awareness raising activities could be key enablers to promote a data protection culture among the general public.

Secondly, DPAs, when explaining rules applicable to controllers, processors and data subjects, do so by taking into account the national law background and specificities. In this way, DPAs contextualise the General Data Protection Regulation to the national context.

Third, awareness raising practices of DPAs, similarly to other enforcers across the EU regulatory domains,[10] allow to mainstream the overall policy objective to the wider audience and in this way minimize disparities in information – the so called information asymmetries – that have been reported among entities, organizations and individuals that process personal data or are subject to the processing operations. For DPAs this task is particularly challenging as on the one hand they must act in order to empower data subjects with control over their personal data, and on the other hand, they have to facilitate data flows within the internal market for controllers and processors.

Finally, the awareness raising duties of DPAs could be seen as a tool reducing divergence in enforcement practices, which if not managed, could potentially result in a forum shopping, where

[7] Robert Baldwin and Martin Cave, *Understanding Regulation: Theory, Strategy, and Practice* (OUP 1999), p. 101.
[8] Article 29 Working Party and the Working Party on Police and Justice joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, The Future of Privacy (2009 WP 168), p. 22-23.
[9] Article 29 Working Party and the Working Party on Police and Justice joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, The Future of Privacy (2009 WP 168), p. 4.
[10] Awareness raising is a horizontal issue that resurfaces across the range of EU policy areas (e.g. national competition authorities; Telecommunications national regulatory authorities etc.).

the concerned entities (i.e. controllers and processors) would look for the most favorable regulatory set-up.[11]

3.4 Awareness raising practices

DPAs reported to use different mediums to reach out the target audience with their awareness raising campaign as well as to learn their distinct needs.[12] DPAs identified the print media, social media and events as the most common general awareness-raising methods. DPAs typically opt-in for the multi-method approach that allows combination of different mediums.

One of the most effective mediums available for DPAs to spread information is their own website. It also could be considered e the most appropriate information platform for the addressees of the information, as they presumably visit the DPAs' websites for information on recent data protection issues, guidelines and decisions. Therefore, the DPAs should be encouraged to share information on decisions, opinions, guidelines, practical examples on data protection, etc. on their website. The information to be provided must be as practical as possible, as especially SMEs reported to be interested in detailed practical information.[13] Arguably, this could be done in coordination with SME associations to avoid duplication of effort and maximise resources. The emphasis here is again on follow-up and mapping the change.

DPAs reported a variety of ways in which they became aware of the needs of SMEs concerning the GDPR. This being said, it should be added that DPAs referred to events as the most effective awareness-raising strategy for SMEs, which also provides better insights into the specific challenges faced by SMEs. The consultation feedback provided by SME representative bodies was mentioned, however, it appeared that the one-to-one interaction that a DPA has with individual SME representatives[14] in a consultation or advisory context provided DPAs with the most substantial benefit in terms of understanding the needs of SMEs. Such interactions reported to occur through established engagement channels such as the public-facing hotline or helpdesk service, participation and presentations at events organised by third parties or other consultation and advisory services. In these contexts, individual SMEs were approaching DPAs with very practical questions that required specific answers. Individual comments made by various DPAs which appear more context specific also help to highlight some other ways in which DPAs can engage at a personal level with SMEs

3.5 An overview of hotlines run by DPAs

The interviews carried out with 18 DPAs by the Consortium on their awareness-raising activities among SMEs about the GDPR concluded that all DPAs operated a form of telephone or email and telephone advice service SMEs can use to contact the DPA. However, in most cases, this service was not an SME specific hotline/helpdesk service.

Overall, it is deemed that a helpdesk or hotline service can be a very useful tool for DPAs to establish connection between the DPA and the general public including the data subjects and SMEs. The interested parties are provided a continuously available source of up to date and trustworthy information. However, a telephone hotline/helpdesk is not always an adequate platform to give legal advice in a specific issue due to liability issues as well as operating an e-mail hotline/helpdesk service can also face the issue of liability, therefore DPAs tend to give general guidance on the data protection legislation.

[11] Kuner C., Bygrave L., Docksey C., The EU General Data Protection Regulation (GDPR): A Commentary (OUP; 2020), 930.
[12] STARII, D.2.1.
[13] STARII, D2.2.
[14] Within the scope of this guidance we consider 'SME representative' to include individuals working for and running SMEs.

It appeared that most DPAs do not use internal guidance to direct hotline/helpdesk advisers (i.e., personnel). Just over a quarter of DPAs did. However, such documents were deemed to be subject to confidentiality and were not shared with the Consortium. Most calls/queries were facilitated in the national language of the respective country which was also the language in greatest demand from SMEs. While some DPAs provided services in multiple languages, English was the most widely used across the EU DPAs in addition to the national language. A small number of DPAs, however, expressed that it would be beneficial to develop their English language capacity in order to respond to the incoming queries.

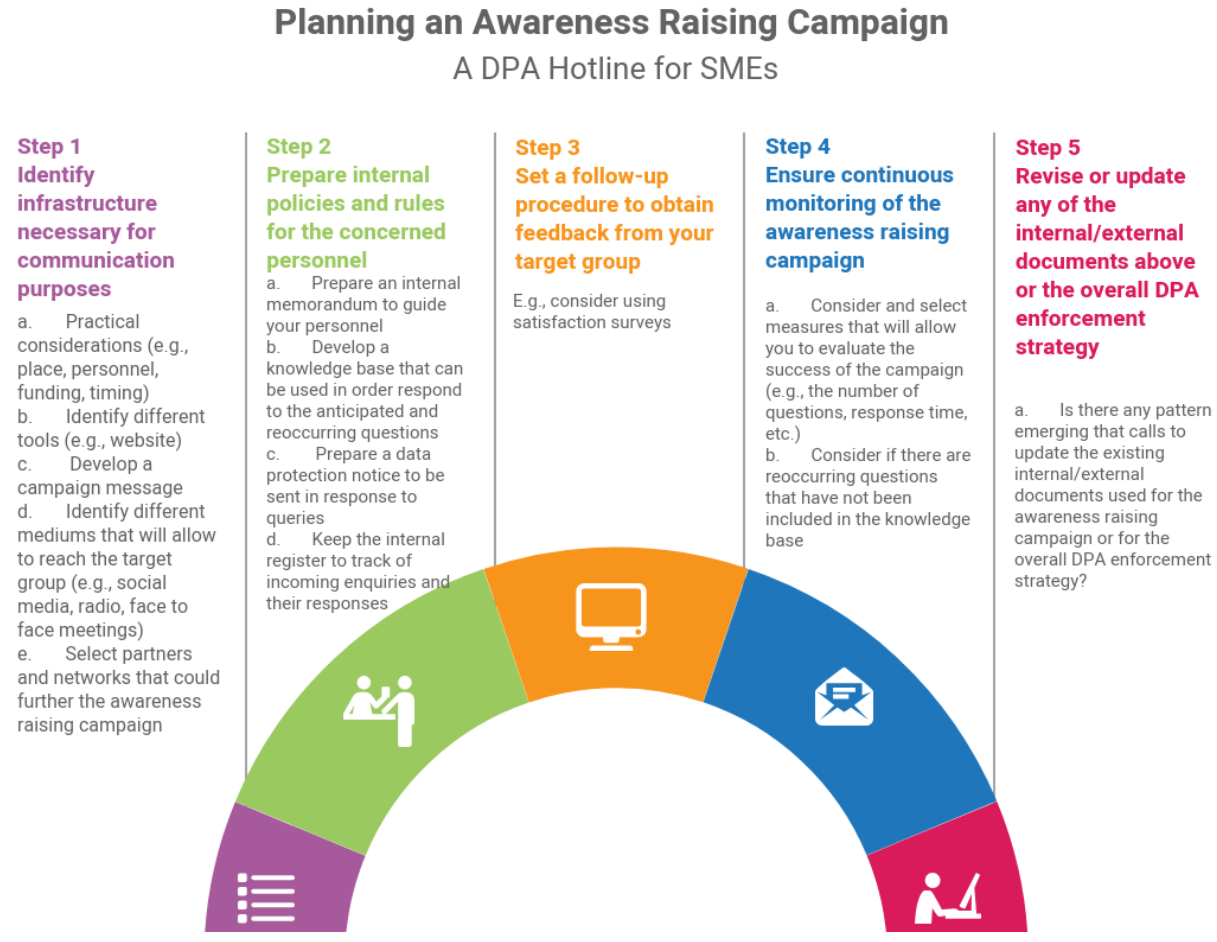
4 NAIH's hotline for SMEs

Within the scope of STARII project, NAIH launched a hotline dedicated to SME enquiries. NAIH operated the hotline between 15 March 2019 and 15 March 2020 in order to assist SMEs with questions and uncertainties concerning compliance with the GDPR. NAIH welcomed questions from SMEs based or functioning across the European Union (EU) about the interpretation and application of the GDPR provisions. This initiative allowed to confirm that indeed a considerable uncertainty remains concerning the application of GDPR provisions, especially, for SMEs. The added value of this initiative is that it allowed to obtain better insights about the specific difficulties and questions SMEs face and that it allowed to draw recommendations on running an awareness raising campaign for a specific target group.

After providing an overview of recommendations, a more detailed description of each of them will be provided in the following sections.

4.1 Recommendations for setting up a hotline for SMEs

After selecting a target group and defining the objective of a particular awareness raising campaign, in our case enhancing GDRP compliance among SME representatives, we believe that by taking the following steps a comprehensive plan for a successful awareness raising campaign, can be developed:



1. **Identify infrastructure necessary for communication purposes**

a. Practical considerations. For an effective set up of the hotline, it is necessary to allocate funding and to find a physical location where this can be run. Personnel to be appointed, either part-time or full time, it has to be trained.
b. Identify different tools. There are several tools through which a hotline can be run. Websites and mail addresses may be the most common tools and effective tools and they were the one chosen by NAHI for running the hotline. Nevertheless, it may be desirable to provide a phone number or a physical address where queries may be sent in paper form to avoid excluding those SMEs with lack of technological literacy.
c. Develop a campaign message in a simple and easy to understand language.
d. Identify different mediums that will allow to reach the target group (e.g., social media, radio, face to face meetings). Even in this case, the medium chosen has to be suitable to avoid excluding part of the populations that may lack digital literacy.
e. Select partners and networks that could further the awareness raising campaign. They can be, for example, sector specific SME associations or networks.

2. **Prepare internal policies and rules for the concerned personnel**. Such policies and rules may include:

    a. Prepare an internal memorandum to guide your personnel. Ideally, people with different seniority will be providing responses in the hotline. Queries received may be divided into different categories according to their complexity and assigned to different officials depending on expertise and seniority level. The memorandum may contain also recommendations concerning the replies, the deadlines for providing answers etc.
    b. Develop a knowledge base that can be used in order respond to the anticipated and reoccurring questions. Ideally, the knowledge base has to be prepared before starting to run the hotline and has to be kept up to date, in the light of the queries received and of the national and European case law developments and issuance of guidance by for example the European Data Protection Board.
    c. Prepare a data protection notice to be sent in response to queries
    d. Keep the internal register to track of incoming enquiries and their responses. Albeit the questions received will feed the knowledge base, it is best practice to ensure the anonymization of the persons forwarding the request.

3. **Set a follow-up procedure to obtain feedback from your target group**

    a. In our case, SMEs who submitted queries concerning personal data processing operations were asked to fill in satisfaction surveys. Setting up a follow up procedure to gather comments and suggestions from users is important to understand how to further improve the hotline.

4. **Ensure continuous monitoring of the awareness raising campaign**

    a. Consider and select measures that will allow you to evaluate the success of the campaign (e.g., the number of questions, response time, etc.). As follow up procedures, continuous monitoring enables to identify the criticalities of the hotline and to correct them.
    b. Consider if there are reoccurring questions that have not been included in the knowledge base. Ideally, every time a new query is presented, it should be included in the knowledge base.

5. **Revise or update any of the internal/external documents above or the overall DPA enforcement strategy**

    a. Consider if there is any pattern emerging that calls to update the existing internal/external documents used for the awareness raising campaign or for the overall DPA enforcement strategy. The results obtained from the hotline could orient DPAs in issues further guidance on recurrent queries.

4.2 Infrastructure for communication purposes

Prior to the launch of the hotline NAIH considered the necessary infrastructure for an awareness raising campaign. This included practical questions concerning the place from where the hotline will be managed and personnel who will be in charge of this task as well as the identification different tools that will be used throughout the campaign (e.g., website page, enquiry form). Then, NAIH in consultation with the consortium partners developed a campaign message that was used to reach out to the target audience. It should be added that NAIH engaged with the target audience different mediums, including social media, radio, and face to face meetings. The latter provide particularly valuable as it allowed to further the awareness raising campaign among the concerned audience.

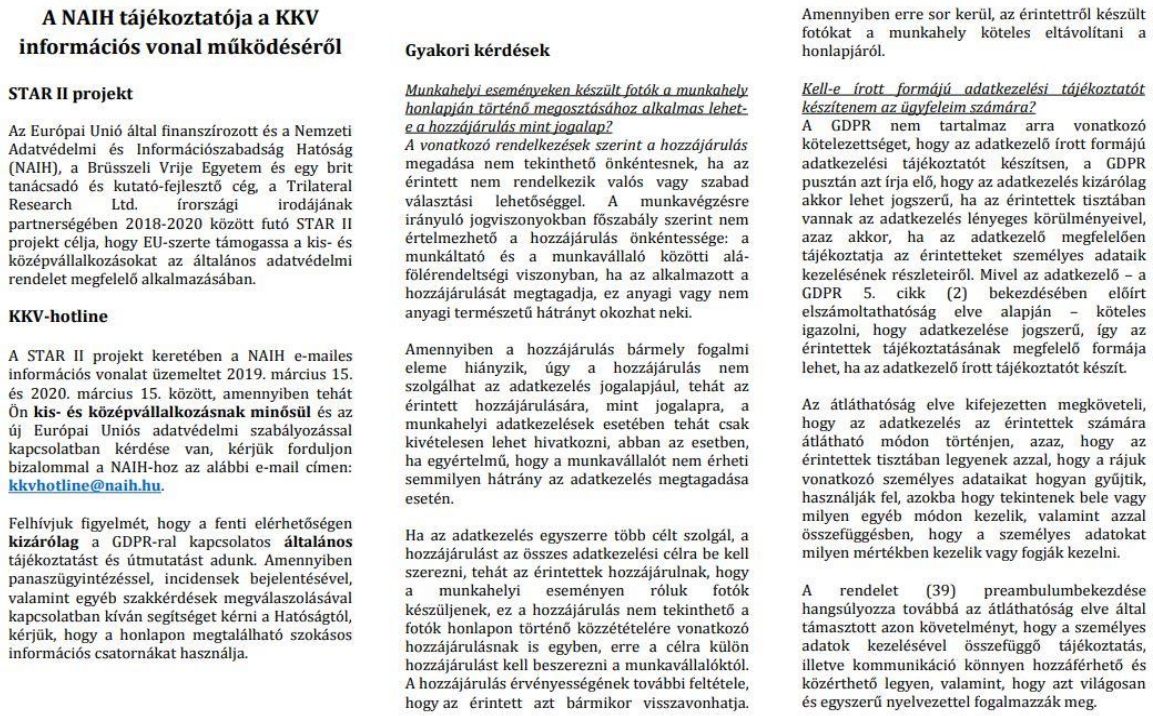
4.2.1 Website

NAIH regularly publishes final decisions and opinions on its website. All available decisions, opinions and recommendations can be searched by topic and are freely available for the public. Considering the engagement with the website and its regular updates with the latest documents issued by the authority, it was decided to create a dedicate part for the awareness raising campaign on this website.

Following up this decision, besides all relevant up to date information on the activity of the authority and general guidance for data controllers and data processors, such as a 12 bullet-point introductory guidance for the GDPR compliance for controllers,[15] the website was updated and now provides information for SMEs on the GDPR compliance via the form of brochure that has been updated on a regular basis. To advertise the STAR II project and the SME hotline the NAIH published an announcement on its website on the launch and operation of the SME hotline on 14.03.2019.

Additionally, the website was used to further spread information on the progress and results of STAR II and especially on the operation of an SME hotline. To this end, the NAIH prepared 2 press releases on the actual status of the project that were published on NAIH's website and also 3 information booklets on the SME hotline (so far). NAIH's website has been considered to be the most appropriate informational platform for the stakeholders of the project as the end-users (i.e. SME representatives) presumably visit the NAIH's website for information on recent data protection issues, guidelines and decisions issued by the authority and other information on the activity of the authority.

[15] See: https://naih.hu/felkeszueles-az-adatvedelmi-rendelet-alkalmazasara.html



A NAIH tájékoztatója a KKV információs vonal működéséről

STAR II projekt

Az Európai Unió által finanszírozott és a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), a Brüsszeli Vrije Egyetem és egy brit tanácsadó és kutató-fejlesztő cég, a Trilateral Research Ltd. írországi irodájának partnerségében 2018-2020 között futó STAR II projekt célja, hogy EU-szerte támogassa a kis- és középvállalkozásokat az általános adatvédelmi rendelet megfelelő alkalmazásában.

KKV-hotline

A STAR II projekt keretében a NAIH e-mailes információs vonalat üzemeltet 2019. március 15. és 2020. március 15. között, amennyiben tehát Ön **kis- és középvállalkozásnak minősül** és az új Európai Uniós adatvédelmi szabályozással kapcsolatban kérdése van, kérjük forduljon bizalommal a NAIH-hoz az alábbi e-mail címen: kkvhotline@naih.hu.

Felhívjuk figyelmét, hogy a fenti elérhetőségen **kizárólag** a GDPR-ral kapcsolatos **általános** tájékoztatást és útmutatást adunk. Amennyiben panaszügyintézéssel, incidensek bejelentésével, valamint egyéb szakkérdések megválaszolásával kapcsolatban kíván segítséget kérni a Hatóságtól, kérjük, hogy a honlapon megtalálható szokásos információs csatornákat használja.

Gyakori kérdések

Munkahelyi eseményeken készült fotók a munkahely honlapján történő megosztásához alkalmas lehet-e a hozzájárulás mint jogalap?
A vonatkozó rendelkezések szerint a hozzájárulás megadása nem tekinthető önkéntesnek, ha az érintett nem rendelkezik valós vagy szabad választási lehetőséggel. A munkavégzésre irányuló jogviszonyokban főszabály szerint nem értelmezhető a hozzájárulás önkéntessége: a munkáltató és a munkavállaló közötti alá-fölérendeltségi viszonyban, ha az alkalmazott a hozzájárulását megtagadja, ez anyagi vagy nem anyagi természetű hátrányt okozhat neki.

Amennyiben a hozzájárulás bármely fogalmi eleme hiányzik, úgy a hozzájárulás nem szolgálhat az adatkezelés jogalapjául, tehát az érintett hozzájárulására, mint jogalapra, a munkahelyi adatkezelések esetében tehát csak kivételesen lehet hivatkozni, abban az esetben, ha egyértelmű, hogy a munkavállalót nem érheti semmilyen hátrány az adatkezelés megtagadása esetén.

Ha az adatkezelés egyszerre több célt szolgál, a hozzájárulást az összes adatkezelési célra be kell szerezni, tehát az érintettek hozzájárulnak, hogy a munkahelyi eseményen róluk fotók készüljenek, ez a hozzájárulás nem tekinthető a fotók honlapon történő közzétételére vonatkozó hozzájárulásnak is egyben, erre a célra külön hozzájárulást kell beszerezni a munkavállalóktól. A hozzájárulás érvényességének további feltétele, hogy az érintett azt bármikor visszavonhatja.

Amennyiben erre sor kerül, az érintettről készült fotókat a munkahely köteles eltávolítani a honlapjáról.

Kell-e írott formájú adatkezelési tájékoztatót készítenem az ügyfeleim számára?
A GDPR nem tartalmaz arra vonatkozó kötelezettséget, hogy az adatkezelő írott formájú adatkezelési tájékoztatót készítsen, a GDPR pusztán azt írja elő, hogy az adatkezelés kizárólag akkor lehet jogszerű, ha az érintettek tisztában vannak az adatkezelés lényeges körülményeivel, azaz akkor, ha az adatkezelő megfelelően tájékoztatja az érintetteket személyes adataik kezelésének részleteiről. Mivel az adatkezelő – a GDPR 5. cikk (2) bekezdésében előírt elszámoltathatóság elve alapján – köteles igazolni, hogy adatkezelése jogszerű, így az érintettek tájékoztatásának megfelelő formája lehet, ha az adatkezelő írott tájékoztatót készít.

Az átláthatóság elve kifejezetten megköveteli, hogy az adatkezelés az érintettek számára átlátható módon történjen, azaz, hogy az érintettek tisztában legyenek azzal, hogy a rájuk vonatkozó személyes adataikat hogyan gyűjtik, használják fel, azokba hogy tekintenek bele vagy milyen egyéb módon kezelik, valamint azzal összefüggésben, hogy a személyes adatokat milyen mértékben kezelik vagy fogják kezelni.

A rendelet (39) preambulumbekezdése hangsúlyozza továbbá az átláthatóság elve által támasztott azon követelményt, hogy a személyes adatok kezelésével összefüggő tájékoztatás, illetve kommunikáció könnyen hozzáférhető és közérthető legyen, valamint, hogy azt világosan és egyszerű nyelvezettel fogalmazzák meg.

4.2.2 Radio campaign

The radio campaign was a vital element in reaching out to the target audience – SME representatives. Radio as the communication channel, the length of the campaign (one month), and the frequency of broadcasting (two plus one spots per day) were based on the previous positive experience gained in the ARCADES project.[16]

The radio campaign raised awareness regarding the data protection obligations by drawing attention to the new regulatory framework concerning the processing of personal data. The campaign also explained the particular form of assistance STAR II will provide. In particular, it referred to the hotline for SMEs and the subsequent recommendations on how to run hotline for other DPAs as well as the handbook for SMEs. A one-month-long campaign with three spots (50 seconds) per day was deemed to be appropriate to deliver the message for a significant number of people, including the target audience.

While there is a good reason to believe that the campaign reached out the target group widely and has increased the GDPR awareness among the SMEs, statistical information on the extent to which such campaign has changed compliance practices and behavior is not available.

NAIH requested quotes from the Hungarian Media Service Support and Trust Fund (MTVA) on the expected costs of the recording and one-month-long broadcast, and later a contract has been signed.

NAIH drafted the text and the scenarios of the radio campaign in English and in Hungarian and then validated them with the consortium. The final text and the scenarios of the radio spot was recorded in Hungarian language on 20.12.2018. The following text was recorded:

"Do you know that small and medium-sized enterprises represent 99% of all businesses in the EU? Rules and obligations of the new EU data protection regulation (coming into force as of May 2018) affect generally these data controllers, too and there are also some specific rules of the GDPR which apply to SMEs. For more information please, contact the National Authority for Data Protection and

[16] See: http://www.arcades-project.eu/index.php.

Freedom of Information, which has set up a special hotline: kkvhotline@naih.hu. This PSA has been prepared upon the request of NAIH and co-financed by the Rights, Equality and Citizenship Programme of the European Union under the supervision of the DG JUST of the Commission."

The radio campaign was broadcasted by Petőfi Rádió, a countrywide available public radio that has the most listeners per day among the entire adult population in Hungary. According to the data published by the National Media and Infocommunications Authority, Petőfi Rádió has had about 1,3 million listeners per day in average in the first quarter of 2019. The radio spot was broadcasted 86 times between 15.03.2019 – 15.04.2019 (17 times in the morning hours, 37 times in the afternoon hours and 32 times in the evening hours).

4.2.3 Face to face interactions

In line with findings of the STARII project, NAIH found face to face interactions to be particularly useful in order to obtain better understanding of SME distinct needs concerning the GDPR compliance. [17]

Within the scope of STARII project, NAIH interacted with SME representative at the following events:

- A validation workshop for the preliminary results of the STARII research project. The event was held in Dublin in June 2019. The report on the first validation workshop can be found in Deliverable D2.3 Report on WP2 Validation workshop.
- An information event for SMEs on the GDPR organized by the Somogy Chamber of Commerce and Industry in June 2019. The Chamber invited the representatives of the NAIH and all SMEs registered at the Chamber. The attending SMEs were provided the opportunity to ask questions they are most interested in concerning the GDPR compliance.
- an information event for SMEs on the GDPR organized by the Budapest Chamber of Commerce and Industry in October 2019. The Chamber invited the representatives of the NAIH and all SMEs registered at the Chamber. The attending SMEs were provided the opportunity to ask questions they are most interested in concerning the GDPR compliance.

Additionally, the President and other representatives of NAIH presented the project and the launch of the SME hotline at several conferences, such as Hungarian Decision maker Think Tank Conference, Infoszféra Conference, Data Protection Case Handling Workshop.

4.3 Internal rules and procedures

After addressing practical considerations, it has proved to be useful to set internal rules and procedures for personnel handling incoming enquiries.

NAIH prepared **an internal memorandum** that laid down the detailed rules for the responses to be given including deadlines, conditions of assistance, liability issues. For example, personnel were required to provide responses in a manner that would provide comprehensible assistance in the interpretation of law applicable relevant to the merit of the question and that would go beyond the mere reference to the provisions of law. Personnel were requested to highlight the relevant aspects in the application of law related to the received question, the factors to be considered among them, and their significance. At the same time, personnel had to ensure that the answer shall contain no opinion as to the lawfulness of any concrete data processing.

NAIH developed the **"knowledge base"** before the launch of the hotline. It included anticipated questions that the DPA expected to receive. The document was updated and revised following up on the statistics provided by the incoming questions and the answers given to them on a monthly basis. More specifically, the Knowledge Base was developed on the basis of the law-enforcement

[17] STARII, D2.1

practice of the Authority and the documents of the European Data Protection Board. The Knowledge Base was prepared in a question–and–answer structure, and contained abridgments of law-enforcement practice in pairs of questions and answers, providing relevant quotations and keywords to assist searches.

NAIH also prepared **a data protection notice**.

To keep track of enquiries, NAIH maintained **the internal register of enquiries**. This allowed to ensure that responses are provided in a timely manner and at the same time it allowed to "tag" and group enquiries and in this way collect statistical data needed for the project. The Register included the e-mail address of the requester as personal data only in order to monitor the fulfilment of the request, and the personal data required for other products by the Project shall be deleted when the SME hotline task is concluded.

4.4 A follow up procedure to obtain feedback

NAIH found it be useful to receive feedback from SMEs who submitted queries concerning personal data processing operations. NAIH decided to do so through the means of satisfaction surveys that were sent by email.

4.5 Continuous monitoring of the awareness raising campaign

The functioning of the SME hotline, the encountered issues and the answers were continuously monitored (qualitatively and quantitatively). Based on the statistical analysis, the functioning of the hotline can be periodically refined and adjusted to the needs. The statistical analysis will also serve as necessary data for the monitoring and evaluation of SME awareness-raising strategies and the success of any knowledge-based resources as well.

As mentioned above, NAIH developed the internal register of enquiries that allowed to keep track of the campaign (e.g., the number of questions, response time, etc.). reoccurring questions that have not been included in the knowledge base

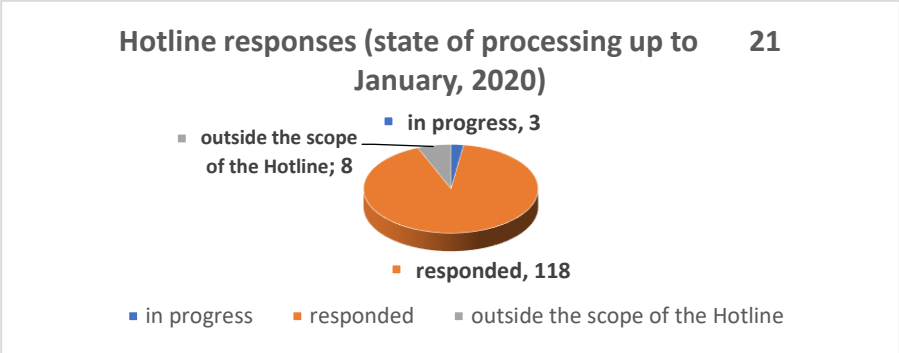
The data obtained from the internal register provided insights about the needs and difficulties SMEs are facing in order to comply with the GDPR. Based on the Register the most frequently asked questions were identified, which was an important indicator of SME concerns and apprehensions about the GDPR.

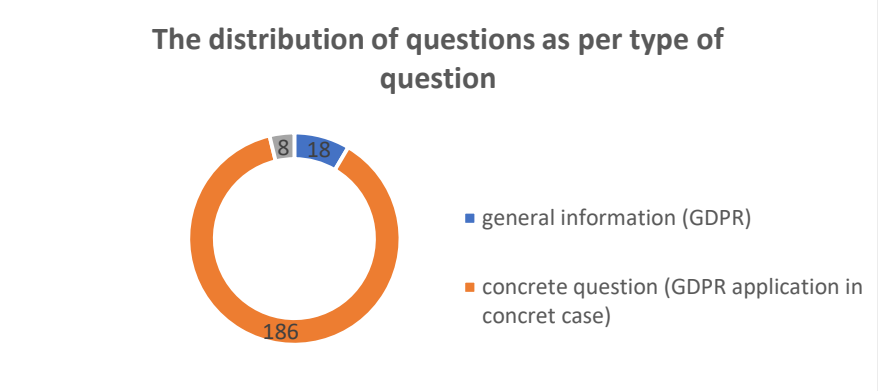
Based on the statistical analysis, the functioning of the hotline was periodically refined and adjusted to the needs of SMEs. The statistical analysis of the data collected in the Register also enabled the DPA to identify the most compelling needs of the SMEs in their compliance and also the assessment of the issues that need to be clarified.

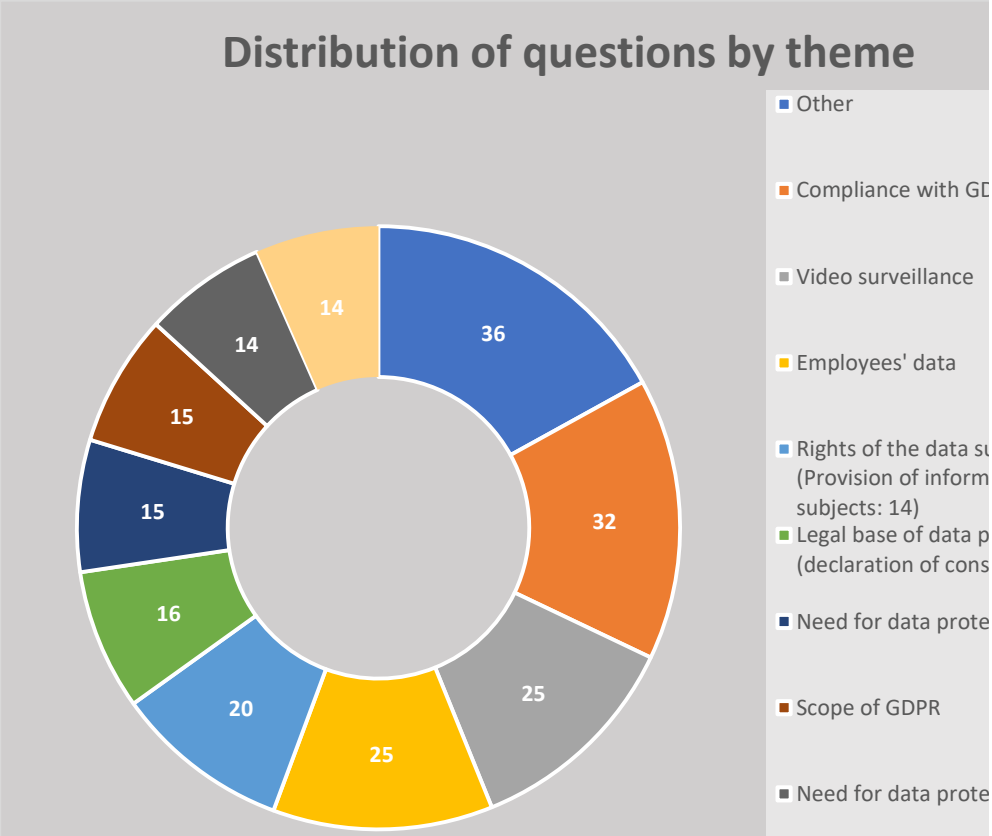
It can be said, that the major outcome of the awareness raising campaign was that encouraged and incentivized the development of the informational strategies that meet the needs of the SMEs representatives. We are included to believe that the statistical data analysis of the hotline can facilitate the customization of the DPA's training program and to monitor changes in SME concerns/queries over time.

Statistical data

The NAIH has experienced a relatively high interest among SMEs during the hotline's operation, but it must be noted that only Hungarian SMEs have used the hotline so far.







5 Concluding remarks

NAIH considers the awareness raising campaign a success as the increased interest of the SMEs on the GDPR compliance was reordered. During the operation of the hotline NAIH had an opportunity to engage with SME representatives through different mediums and found that the majority of the SMEs that sent enquiries learned about the campaign after finding a notice on the website of NAIH; a smaller part referred to the radio campaign.

While the NAIH was able to draw some recommendation of best practices concerning the set-up of a hotline for SMEs, it recognises that each DPA is independent in it actions as they concern fulfilment of the leader orientated obligations stemming from Article 57 of the GDPR, such as the ones highlighted in bold.

Article 57

Tasks

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

(l) give advice on the processing operations referred to in Article 36(2);

(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);

(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

(p)draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(q)conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(r) authorise contractual clauses and provisions referred to in Article 46(3);

(s) approve binding corporate rules pursuant to Article 47;

(t) contribute to the activities of the Board;

(u)keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and

(v) fulfil any other tasks related to the protection of personal data.

6 Part B – Handbook for SMEs

6.1 Methodology

Recognizing that legal uncertainty over GDPR application remains relatively high among European enterprises, and especially SMEs,[18] this handbook unpacks the meaning of the GDPR provisions entailing a risk-based approach. A core message coming through from the STAR II data is that SMEs face a methodological challenge with the GDPR in the sense that they understand it conceptually but less so how it applies to their specific context.

This specific methodology has been chosen as a result of findings extracted during interviews conducted with 18 DPAs, 22 SME association representatives, 52-60 respondents to the online survey and 11 face to face interviews with SME representatives that were conducted within the scope the STAR II research in 2019.[19] Additionally, the handbook aims at integrating other four recommendations, which were most frequently suggested from the respondents within the scope of interviews conducted by the Consortium partners.[20] In particular, respondents suggested that the handbook should be:

1. A generic SME handbook focused predominantly on a compilation of examples and templates.
2. A sector specific handbook.
3. 'Selling' the GDPR handbook.
4. Myth-busting handbook.

The consortium decided to follow a holistic approach in the handbook and consider five most popular suggestions that emerged during interviews as they appeared to be supplementary and facilitating GDPR compliance for SMEs. This approach also allows to address the needs of various SME types.

The handbook is structured in a way that it firstly introduces background of a provision and only then it is going to provide references to good practices, include examples, and references to templates that have been developed by the DPAs. To some extent we will also rely on the guidance provided by WP29, that has been replaced by the EDPB. The added value of this handbook is that it provides a reference point for SMEs seeking to understand the risk-based approach. Furthermore, we are inclined to be believe that different parts of this document are going to be useful for different SMEs.

6.2 DPAs guidance on GDPR compliance for SMEs

To enhance compliance with the revised EU data protection framework, DPAs independently and in the set-up of the European Data Protection Board (EDPB) have been issuing guidance on various aspects concerning the GDPR. Some of such guidance documents have been addressed to SMEs.

Based on the information provided by the STAR II DPA interviews as well as desktop research of all EU DPA websites, it appears that slightly less than one third of EU DPAs currently provide GDPR guidance that is specifically tailored for SMEs; upon last review this included the DPAs from

[18]

[19] STARII, Deliverable D2.1 Report on DPA efforts to raise awareness among SMEs on the GDPR (Version 1.1; 2019); STARII, Deliverable D2.2 Report on the SME experience of the GDPR (2019).

[20] Add a link to D2.1 and D.2.2.

Belgium (APD),[21] France (CNIL),[22] Ireland (DPC),[23] Lithuania (VDAI),[24] Slovenia (IP),[25] Spain (AEPD),[26] Sweden (Datainspektionen)[27] and the UK (ICO).[28] Some of these DPAs further distinguish guidance for micro-businesses.[29]

The guidance provided through the DPA websites and takes the form of either a downloadable document, a section of the DPA website or indeed a separate dedicated website. The approach taken in the SME specific guidance is usually holistic in terms of the issues covered, often presented in the same order as an SME might logically need to commence addressing data protection within their organisation. The issues typically include, in various presentation styles: key concepts of the GDPR (e.g. what is (not) personal data and the difference between personal data and special categories or the so called sensitive data), principles (e.g. accuracy, data minimisation, limited retention); data security obligations concerning technical and organisational set up of the processing; obligations concerning data subject rights; and the appointment of a Data Protection Office (DPO), among others. These issues were often usefully identified to SMEs by the asking of positive questions or activity-based steps rather than approaching the issue in terms of the GDPR obligations.

Apart from guidance documents for SMEs, DPAs across the EU have reported to engage in numerous awareness raising activities.[30]

6.3 The concept of a risk-based approach in the EU data protection framework

The articulation of the risk-based approach has led to the principal novelties of the EU data protection framework. By providing more substance to the previously established principles, the risk-based approach aims to bring compliance from theory to practice. It is embedded in Article 24 on responsibility of the controller, Article 25 on data protection by design and by default, Article 30 on the obligation for documentation, Article 31 on the notification to DPAs, Article 32

[21] The Belgian Data Protection Authority operates in a number of languages. *L'Autorité de protection des données* (APD) is the French abbreviation simply translates as Data Protection Authority in English. CPVP, 'RGPD Vade-Mecum Pour Les PME (January)' (2018) <https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/PME_FR_0.pdf>.

[22] *La Commission Nationale de l'Informatique et des Libertés* (CNIL) meaning the National Commission of Information Technology and Freedoms. See, Bpifrance, 'Guide Pratique de Sensibiliation Au RGPD (April)' (CNIL 2018) <https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf>.

[23] *An Coimisiúm um Chosaint Sonrai/* The Data Protection Commission (DPC). See, 'Guidance Note: GDPR Guidance for SMEs (July)' (Data Protection Commission 2019) <https://www.dataprotection.ie/sites/default/files/uploads/2019-07/190708 Guidance for SMEs.pdf>.

[24] *Valstybinė duomenų apsaugos inspekcija (VDAI)* meaning State Data Protection Inspectorate. See, VDAI, 'Rekomendacija Smulkiajam Ir Vidutiniam Verslui Dėl Bendrojo Duomenų Apsaugos Reglamento Taikymo (September)' (2018) <https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_SVV_BDAR_2018.pdf>.

[25] Informacijski pooblaščenec (IP) meaning the Information Commissioner. See, 'Varstvo Osebnih Podatkov' (*Upravljavec*, 2018) <https://upravljavec.si> accessed 3 October 2019.

[26] Agencia Española de Protección de Datos (AEPD) meaning Spanish Data Protection Agency. See, 'Facilita RGPD' (*AEPD*) <https://www.aepd.es/herramientas/facilita.html> accessed 3 October 2019.

[27] Meaning Data Inspection Board. See, 'GDPR - Nya Dataskyddsregler' (*Verksamt*, 2018) <https://www.verksamt.se/driva/gdpr-dataskyddsregler> accessed 3 October 2019.

[28] Information Commissioner's Office (ICO). See, 'Micro, Small and Medium Organisations' (*ICO*) <https://ico.org.uk/for-organisations/in-your-sector/business/> accessed 3 October 2019.

[29] 'Guidance Note: Data Security Guidance for Microenterprises (July)' (Data Protection Commission 2019) <https://www.dataprotection.ie/sites/default/files/uploads/2019-07/190709 Data Security Guidance for Micro Enterprises.pdf>; 'How Well Do You Comply with Data Protection Law: An Assessment for Small Business Owners and Sole Traders' (*ICO*) <https://ico.org.uk/for-organisations/data-protection-self-assessment/assessment-for-small-business-owners-and-sole-traders/> accessed 4 October 2019.

[30] See, Contribution of the EDPB to the evaluation of the GDPR under Article 97, Adopted on 18 February 2020, 35-46.

on security of processing, Articles 33 & 34 on personal data breach notifications, Article 36 on the obligation to carry out an impact assessment, and Article 36 on prior consultation.[31]

While the formulation of the risk-based approach to some degree varies in the above listed articles, in essence, it aims to ensure that **whatever the level of risk involved in the processing of personal data, data subjects' rights are respected**. From the pragmatic compliance point of view, some suggest that the risk-based approach requires '**adjusting some of the data protection obligations to the risks presented by a data processing activity**'.[32]

It is important to note that there are different approaches that could be taken in order to unpack the meaning of the concept of a risk-based approach in the GDPR.

One of them would include turning to regulatory theories that may seem to be ground-breaking as they offer the semantics of risk that have been foreign to the legal vocabulary until rather recently. Ulrich Beck, the renowned scholar, whose writings shaped the contemporary understanding of risk, notes 'that we are living in a world risk society not only in a sense that everything is being transformed into decisions whose consequences are unforeseeable or in the sense of risk management societies or risk discourse societies'.[33] Building on this observation it is no surprise that the term 'risk' has entered the legal domain. It should be pointed out that because the term 'risk' has been indeed more frequently used in the areas concerning technology, economics, natural sciences and politics, its understanding in law is still evolving.[34] In view of this, it may be useful to consider different typology of risks pointed out by Robert Baldwin and Martin Cave in their seminal work on understanding regulation. They note that risks can be 'subjective'[35] and 'objective' [36] as well as voluntarily undertaken, [37] societally imposed, [38] discrete and pervasive[39]; any of such risks can be evaluated from different perspectives (e.g., technological, economics, psychological).[40] In fact, the perception of risk, as is well pointed out in the seminal work of social scientist Paul Slovic, is affected by different attitudes, the manner in which information is given and portrayed, and the familiarity of the person with an activity or hazard.[41] In particular, Slovic suggests that the following elements play a role when evaluating risk:

1) The degree they feel in control;
2) The nature of consequences, the distribution of the impact;
3) Whether they are exposed to an activity voluntarily;
4) The perceived the benefits of activity.[42]

While these insights are without a doubt very interesting, they are of little use as far as the legal analysis and the interpretation of the term 'risks' in the GDPR are concerned. To aid this situation, it is reasonable to turn to guidance and opinions issued by the regulators in the set-up of the Article 29 Working Party. The notion of 'a risk' drew attention by the regulators during the data protection reform, which introduced the so-called risk-based approach.[43] This approach is not entirely new, and its origins can be traced to the Data Protection Directive – security

[31] Also, Article 37 on designation of the data protection officer and Articles 40 and 42 on the use of certification and codes of conduct are of relevance for SMEs.

[32] Kuner C., Bygrave L., Docksey C., The EU General Data Protection Regulation (GDPR): A Commentary (OUP; 2020), p.26
[33] Ulrich Beck, *World at Risk* (Polity 2009) 14–15.
[34] ibid 6.
[35] Subjective risk assessment entails non-expert perceptions by the public.
[36] Objective risk is assessed scientifically by experts and is probabilistic.
[37] For example, by taking some drugs, such as contraception.
[38] For example, a nuclear power plant.
[39] The latter includes risks that are bound to happen, such as an earthquake.
[40] Robert Baldwin and Martin Cave, *Understanding Regulation: Theory, Strategy, and Practice* (Oxford University Press 1999) 139.
[41] P Slovic, 'Perception of Risk' (1987) 236 Science 280–285.
[42] ibid.
[43] Raphaël Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279 <https://www.sciencedirect.com/science/article/pii/S0267364917302698> accessed 11 April 2018.

requirements, the DPA prior notification and treatment of sensitive categories of data, respectively foreseen in Articles 17, 20 and 8.[44]

The risk-based approach is **easy to spot** in the text of the GDPR, nonetheless its practical application still raises practical and theoretical concerns. The WP 29 suggests that '**a "risk" is a scenario describing an event and its consequences, estimated in terms of severity and likelihood**.'[45] Despite this definition reiterating the conventional understanding of risk in the literature, it raises uncertainty as there is no one methodology to follow to evaluate risk.[46] An action that should be taken by both controllers and processors is defined by the regulators as "risk management", which is perceived 'as the coordinated activities to direct and control an organization with regard to risk'.[47]

While in general risk is understood as a future threat, in data protection law, it relates more specifically to **threats concerning the rights and freedoms of individuals** whose personal data are being processed. The WP29 made it clear on several occasions, that such threats are not limited to the right to protection of personal data or privacy. In particular, it has argued that in the statement concerning risk based approach and the Opinion concerning data protection impact assessments that while 'the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy… [it] may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.'[48] Consequently this means that for each processing the relevant rights and freedoms of individuals must be considered. The consideration of potential threats must be carried out on individual basis, therefore, must take into account the context of the processing.

6.3.1 Risk-based approach formula

Typically, the risk-based approach formula in the GDPR includes the following elements:

- taking into account;
- the state of the art ... of the means for processing;
- the cost of implementation;
- the nature, scope, context of processing;
- purposes of processing; and
- risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

6.3.2 Types of risks

While evaluating risks to rights and freedoms may be troublesome in some contexts for data controllers, the following three types of risks are distinguished for compliance purposes:

1) low risk situations, where the risk to data subjects is minimal and a controller may be exempt from some GDPR requirements. For example, a notification of a personal data breach to DPA or individuals may not be necessary.

---

[44] Article 29 Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (2014) 2.
[45] Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (2017) 6.
[46] Raphaël Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279 <https://www.sciencedirect.com/science/article/pii/S0267364917302698>.
[47] Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (2017) 6.
[48] ibid.

2) risky situations, where personal data are processed and requires controllers (and processors) to take appropriate organisational and technical measures.

3) high risk situations, where controllers because of undertaking activities involving "high-risk" are required to take additional measures, such conducting a data protection impact assessment or consulting a data protection authority prior to launching a processing operation.

It is important to establish the threshold for each category of risk as it can trigger the application of certain provisions.

6.3.3 How can a risk-based approach benefit SMEs?

The EDPB provides the following conceptualization of a risk-based approach:[49]

> The risk and the assessment criteria are the same: the assets to protect are always the same (the individuals, via the protection of their personal data), against the same risks (to individuals' rights and freedoms), taking into account the same conditions (nature, scope, context and purposes of processing).

This definition is important to consider for SMEs because it makes it clear that risks for data subjects do not depend on the size of the controllers. It is important to note that, however, the risk-based approach benefits SMEs. As suggested by European regulators on several occasions, the risk-based approach may include the use of baselines, best practices and standards. These might provide a useful toolbox for controllers to tackle similar risks in similar situations (nature, scope, context and purpose of processing).

Considering compliance with the GDPR through the lens of a risk-based approach is particularly useful for SMEs for two reasons.

- First, following this approach SMEs are required to engage in a continuous balancing act and consider whether personal data processing operations may result in (high) risk situations and what are measures that an SME can implement to mitigate such (high) risks.
- Second, the risk-based approach allows for SMEs to frame data protection requirements in a flexible manner. It does not prescribe or demand a particular measure but instead it requires to understand the processing by considering its nature, scope, context and purpose as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons whose personal data are being processed.

6.3.4 Attribution of roles

It is established by the case law of the Court of Justice of the EU (CJEU) and WP29 guidance that the determination of whether an entity is a controller or a processor for the purposes of EU data protection law is a key element in the assessment of the application of the GDPR to the processing of personal data in question. Under the EU data protection framework, **controllers bear an ultimate responsibility for the processing of personal and for complying with the key data protection requirements and principles**, which include: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality (security), and accountability.

The GDPR provides the following definition:

[49] EDPB, Guidelines 4/2019on Article 25 Data Protection by Design and by Default, Adopted on 13 November 2019,9.

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (Article 4 (7)).

6.3.5 Accountability

(a) Background

The concept of accountability is relevant for different types of SMEs and enterprises across various sectors. A definition that has been widely recognised originates from the governance scholar, Bovens, defining accountability as both a virtue that entails "a normative concept, as a set of standards for the behaviour of actors, or as a desirable state of affairs" and as a mechanism "that involves an obligation to explain and justify conduct".[50] An example of such a mechanism could be an obligation to demonstrate that the processing of personal data is in compliance with the EU Data Protection Framework.

In the field of data protection and privacy, "accountability is [considered to be] a form of enhanced responsibility"[51] and the actual recognition of the principle within the GDPR marks a shift from a primarily reactive approach to a proactive compliance and practice. As per Alhadeff, Van Alsenoy and Dumortier, accountability is "a proactive demonstration of an organization's capacity to comply has the potential of improving the current state of the art in two ways: 1) transparency and confidence for both regulators and data subjects, and 2) greater transparency of corporate practices".[52]

(b) What does SMEs need to do to be accountable?

To be accountable a controller must adopt policies and implement appropriate measures to ensure, and be able to demonstrate, compliance with the data protection framework. More specifically, according to Article 24 of the GDPR, the controller is responsible for implementing appropriate technical and organisational measures to ensure and to demonstrate that its processing activities are compliant with the requirements of the GDPR. When taking such measures, the controller has to take into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

The assessment and evaluation of the risks associated with the processing of personal data should serve to enhance transparency practice of written policies and documentation. Therefore, it can be observed that the principle of accountability as an elements of good governance may benefit data subjects and businesses.

(c) What are the examples of accountability measures?

[50] Bovens, M.: Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism, West European Politics, 946 — 967 (2010)

[51] Bennett, C.: The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats. In Guagnin, D., Hempel, L., Ilten, C., Kroener, I., Neyland, D., Postigo H. (eds.), Managing Privacy through Accountability, Springer (2012) 46

[52] Alhadeff, J., Van Alsenoy, B., Dumortier, J.: The accountability principle in data protection regulation: origin, development and future directions. In Guagnin, D., Hempel, L., Ilten, C., Kroener, I., Neyland, D., Postigo H. (eds.), Managing Privacy through Accountability, Springer (2012)

Examples of documents and actions that facilitate demonstration compliance with this obligation include adopting and implementing data protection policies; taking a 'data protection by design and default' approach; putting written contracts in place with organisations that process personal data on your behalf; maintaining documentation of your processing activities (see Article 30); implementing appropriate security measures; recording and, where necessary, reporting personal data breaches; carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests; appointing a data protection officer; and adhering to relevant codes of conduct and signing up to certification schemes.

It should be noted that these measures need to be continuously revised and updated in order to reflect the processing operations. Consequently, this means that accountability obligation requires a continuous effort from the controller's side.

6.3.6 Data protection by design and data protection by default

(a) Background

Data Protection by Design and Data Protection by Default (DPbD and DPbDf) left the realm of 'buzzwords' and entered the one of legal obligations, once the European General Data Protection Regulation[53] (GDPR) was adopted in 2016. The importance of these principles has grown in proportion to the deadline for the GDPR implementation and the fears over looming fines.

The underlying objective of DPbD and DPbDf obligations is to integrate privacy throughout the lifecycle of various technologies and applications that process personal data. At the same time, the practical implementation of DPbD and DPbDf is tremendously complex because of the uncertainty shielding the meaning of these principles.[54]

(b) What does data protection by design entail?

The principle of data protection by design requires the data controller to implement both organisational and technical measures in order to ensure that the requirements of the GDPR are embedded in the processing activity, in an effective manner, at the time of initiating it as well as at its later stages. The data controller has to do so by taking into account the nature, scope and context of processing and other criteria detailed in the provision. In particular, the controller must

- implement appropriate technical and organisational measures and necessary safeguards into the processing;
- implement data protection principles (see Article 5) and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects (see Chapter III);
- in an effective manner;
- at the time of the determination of the means for processing and at the time of the processing itself.

(c) How to measure effectiveness of data protection by design measures?

In its opinion the EDPB notes that **effectiveness** means that controllers: **must be able to demonstrate** that they have implemented dedicated measures to protect data protection

[53] European Parliament and the Council, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[54] Michael Veale, Reuben Binns and Jef Ausloos, 'When data protection by design and data subject rights clash' (2018) International Data Privacy Law, ipy002, https://doi.org/10.1093/idpl/ipy002.

principles, and that they have integrated specific safeguards that are necessary to secure the rights and freedoms of data subjects.

It is therefore not enough to implement generic measures solely to document DPbDD-compliance; each implemented measure must have an actual effect.

While Article25 does not oblige controllers to implement any prescribed technical and organizational measures or safeguards, the measures and safeguards chosen by controllers should be designed to be robust and be able to be scaled up in accordance with any increase in risk of non-compliance with the principles.

In order to demonstrate compliance, controllers may opt in for the use 'key performance indicators to demonstrate compliance. Key performance indicators may include metrics to demonstrate the effectiveness of the measures in question. Metrics maybe quantitative, such as level of risk, reduction of complaints, reduction of response time when data subjects exercise their rights; or qualitative, such as evaluations of performance, use of grading scales, or expert assessments. Alternatively, controllers may provide the rationale behind their assessment of the effectiveness of the chosen measures and safeguards.'

(d) What does data protection by default entail?

A "default", as commonly defined in computer science, refers to the pre-existing or preselected value of a configurable setting that is assigned to a software application, computer programor device. Such settings are also called "presets" or "factory presets", especially for electronic devices. 40.Hence, "data protection by default" refers to the choices made by a controller regarding any pre-existing configuration value or processing option that is assigned in a software application, computer program or device that has the effect of adjusting, in particular but not limited to, the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

(e) What are the examples of measures implementing data protection by default?

Access control policies are perhaps one of the most illustrative examples of how to implement data protection by default in practice. Following this principle, the controller must limit who can have access to personal data based on an assessment of necessity, and also make sure that personal data is in fact accessible to those who need it when necessary, for example in critical situations.

Access controls must be observed for the whole data flow during the processing. Personal data should not be made accessible, without the individual's intervention, to an indefinite number of natural persons.

6.3.7 Documentation

(a) Background

Documentation may be regarded as further continuation of the accountability obligation stemming from Article 24. The WP29 highlights that the record of processing activities is a very useful means to support an analysis of the implications of any processing whether existing or planned. The record facilitates the factual assessment of the risk of the processing activities performed by a controller or processor on individuals' rights, and the identification and implementation of appropriate security measures to safeguard personal data – both key components of the principle of accountability contained in the GDPR.

For many micro, small and medium-sized organisations, maintaining a record of processing activities is unlikely to constitute particularly heavy burden.

(b) What does documentation require?

According to Article 30, data controllers are required to keep records of their processing activities. When discussing the documentation obligation alternative terms are being used, including but not limited to, an inventory, a register, and a data management plan. Upon request, these records must be disclosed to the national data protection authority (DPA). Keeping accurate documentation of processing activities can be useful for an entity if it needs to demonstrate compliance for DPA.

European data protection regulators explain that documentation of processing activities must be kept in writing.[55] The controller (and the processor) can chose whether to keep such records in paper or in an electronic form. It is assumed that organisations will, however, benefit more from maintaining their documentation electronically as such documentation can they can easily add to, remove, and amend it as necessary. Paper documentation is regarded appropriate for SMEs and micro enterprises. It should be added SMEs (entities having less than 250 employees) are exempt from this obligation if:

- processing that is likely to result in a risk to the rights and freedoms of data subjects;
- processing that is not occasional (meaning that it is regular); or
- processing that includes special categories of data or personal data relating to criminal convictions and offences.

This exemption does not apply to SMEs when processing personal data in the context of activities that are going to involve continuous processing of personal data. Finally, it should be noted that multiple templates and specialist software packages facilitating documentation are available on the market. Examples of free templates are provided by data protection regulators; they can be available on the websites of the following DPAs: ICO, Belgian DPA and CNIL.

The documentation should include information about the following:

- the name and contact details of the controller/representative/ DPO;
- the purpose/s of the processing;
- the categories of data subjects and personal data processed;
- the categories of recipients with whom the data may be shared;
- information regarding international data transfers;
- where possible, the applicable data retention periods; and
- where possible, a description of the security measures implemented in respect of the processed data.

6.3.8 Appointment of the DPO

(a) Is appointment of a DPO mandatory for SMEs?

The appointment of a Data Protection Officer (DPO) regards both **data processors** and **data controllers** and it is mandatory only in certain cases:

[55] Based on the opinions and guidance provided by the UK DPA (ICO), the French DPA (CNIL) and the Irish DPA.

1) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity

Normally, this situation does not regard SMEs, but it may be possible that an SME is entrusted, under the legal regime applicable to it, with the performance of services of public interest (e.g. public transport services, water and energy supply, road infrastructure, public service broadcasting, public housing etc.). In this case, it shall appoint a DPO.

2) the core activities of the SME consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale

Core activities of an SME refer to the main business pursued by the business. It may be that the core activity of the SME is inextricably linked with data processing (e.g. if the SME is providing a surveillance service for a shopping centre and has to monitor CCTV cameras). At the same time, certain data processing activities, albeit essential or necessary to a business, are considered ancillary (e.g. paying employees or having standard IT support activities).

Activities that may constitute a regular and systematic monitoring of data subjects include e.g. operating a telecommunications network; providing telecommunications services; email retargeting; data-driven marketing activities; profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering); location tracking, for example, by mobile apps; loyalty programs; behavioural advertising; monitoring of wellness, fitness and health data via wearable device.

Large-scale activities encompass processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards); processing of real time geo-location data for statistical purposes by a processor specialised in providing these services.

3) the core activities of the SME consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

Examples: SME is involved in health-related sector (e.g. laboratories that provide blood analysis), criminal law firms; SME providing dating app services etc. will have to appoint a DPO.

Important note: the above-mentioned cases in which the appointment of a DPO is mandatory regard only GDPR provisions. It may be possible that the national laws implementing the GDPR foresee other situations in which this is mandatory.

(b) Who should be a DPO?

A DPO may either be an **employee of the SME** or an **external expert**, but in both cases, it is fundamental that he or she is **independent**, in the sense that:

- the DPO shall be provided of all the necessary resources to carry on his/her tasks, in terms of money, time, workforce, time to devote to professional development etc.;
- the DPO shall not receive instructions for the exercise of his/her tasks;
- the DPO shall not dismissed or penalized for the performance of his/her tasks;
- the DPO shall report to the highest management; and
- the DPO should not be in conflict of interest in respect to other tasks and duties (e.g. determining objects and purposes of the processing, representing the SME in legal proceeding).

In the light of the above, at practical level, when a DPO is an employee of the organisation, it must be made clear if he or she is acting in the DPO function or not.

As regards the level of expertise, it must be commensurate with the sensitivity, complexity and amount of data an organisation processes. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a

higher level of expertise and support. The GDPR neither imposes an obligation for certification of a DPO nor does it encourage such certification on a voluntary basis.

(c) What tasks can be assigned to a DPO working for SMEs?

Task of DPOs	DPOs cannot
Inform and advice the SME on the obligations arising from the GDPR and the national data protection provisions	Be held accountable for the information and advice given to the SME
Monitor the compliance of the SME with the GDPR, the national data protection provisions and (eventual) its internal data policies	Be considered personally responsible for non-compliance with data protection requirements
Carry on awareness raising activities and training for the staff of the SME dealing with data processing	Perform the DPIA
Provide advice to the SME and monitor the performance in relation to the DPIA (when a DPIA is required)	Represent the SME in front of the DPA or in a court in case of proceedings
Act as contact point for the supervisory authority in case of prior consultation	Be considered responsible for the maintainance of the register
Cooperate with the supervisory authority	
Be contacted by data subjects willing to exercise their rights	
Create and maintain the register of processing (in the exceptional situations where SME are required to have it)	

(d) Can I share my DPO with other organisations?

Appointing a joint DPO may be a practical solution for a group of SMEs. It is a possibility foreseen by the GDPR, on condition that:

- The DPO is easily accessible from each establishment. The notion of accessibility refers to the tasks of the DPO as a contact point with respect to data subjects, the supervisory authority and also internally within the organisation.

(e) What should SMEs consider before appointing a DPO?

- Not all the SMEs have to appoint a DPO, but it still may be useful to have an expert in data protection working within the enterprise and dealing with stakeholders. It arguably may result in a competitive advantage.
- When the SME is entrusted, under the legal regime applicable to it, with the performance of services of public interest, albeit it is not mandatory, it is recommended that the SME designates a DPO.
- To be able to demonstrate compliance (accountability) with the regulation, it may be useful to document why the enterprise chose to appoint or not to appoint a DPO, and why his/her level of expertise was deemed appropriate required.
- To be able to demonstrate compliance (accountability) with the regulation, when a SME decides to pursue an activity in contrast with the advice of the DPO, it should document the reasoning.

Risks for non-compliance: infringements relating to the appointment of a DPO can be subject to administrative fines up to 10,000,000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

6.3.9 Data Protection Impact Assessment

(a) Background

The DPIA is a new addition to the EU data protection framework. It builds on the rich experience of conducting impact assessments in other fields, in particular, on the environmental impact assessments. To be effective, impact assessments are carried out at the early stage of a project (proactive initiative), at the phase of planning or designing, and are aimed to anticipate the potential beneficial and adverse (i.e. negative) impacts of such project. Impact assessments help decision-makers find the best and most beneficial solutions for the development and deployment of initiatives.[56] To be practical, impact assessments must be scalable, flexible and applicable inter alia for large organisations, consortia or for small and medium-sized enterprises.

(b) When is a DPIA mandatory?

Article 35 of the GDPR lists several conditions when

Article 35.3 of the GDPR, makes it clear that there are some situations that by their own nature entail high risks to rights and freedoms of individuals, and thus require a DPIA, namely:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.[57]

[56] E.g. environmental impact assessments originated from green movements in the 1960s (read more at: International Association for Impact Assessment: Principles of Environmental Impact Assessment Best Practice <https://www.eianz.org/document/item/2744> [07/05/2016]) and social impact assessments (SIA) were developed in the 1980s. SIAs aim at ensuring that developments or planned interventions maximise the benefits and minimise the costs of those developments, including, especially, costs borne by the community (for more information read: The Interorganizational Committee on Guidelines and Principles for Social Impact Assessment: Guidelines and Principles for Social Impact Assessment <http://www.nmfs.noaa.gov/sfa/social_impact_guide.htm> [07/05/2016])

[57] European Union Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ EC (GDPR) (n 36) Article 35.3.

(c) What are the elements and characteristics of the processing may generate the high risks to rights and freedoms of individuals?

The following elements that contribute to the high risk from this provision were extracted by the WP29, in particular: 1) evaluation or scoring, including profiling and predicting, 2) automated-decision making with legal or similar significant effect, 3) systematic monitoring, 4) sensitive data or data of a highly personal nature, 5) data processed on a large scale, 6) matching or combining datasets; 7) data concerning vulnerable data subjects, 8) the use of innovative or new technological or organisational solutions, 9) situations where the processing in itself "prevents data subjects from exercising a right or using a service or a contract."[58] These elements are not cumulative and it is suffice for one of them to be present to create a high risk for data subjects.[59] However, the WP 29 warns that these elements that could be used to determine the threshold for distinguishing risk into 1) a risk and 2) a high risk when determining the need for a data protection impact assessment are not applicable when considering whether a controller has an obligation to notify a data breach to individuals

(d) What situations could require a DPIA?

Examples of processing operations that could trigger a DPIA:

- If the SME is implementing a new tool to monitor access to office combining use of fingerprints and face recognition;
- If the SME is a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks
- If the SME is providing CCTV surveillance shopping centre
- If the SME is processing data of vulnerable people (e.g. employees, children, minorities etc.)
- If the SME is performing creditworthiness assessment on the basis of automated decision making
- If the SME is monitoring social media data to create profiles

(e) Who and when should perform a DPIA?

Albeit the data processor and the data protection officer shall assist the data controller (i.e., SME), the final responsibility on the DPIA process relies on the data controller.

In principle, the data protection impact assessment process has to start *before* the starting of the data processing operations because it has been conceived as a tool to inform the decision-making concerning the envisaged processing operation, in order to minimise the data protection risks connected to it. But it can also be performed later (if there is a change in the risk related to the processing operations, determined e.g. by the introduction of a new technology or new purposes of processing).

A DPIA can also be useful for assessing the data protection impact of a technology product (e.g. if the SME is developing a piece of hardware or a software, or offering data shredding and sanitizing services or cloud based storage).

(f) When DPIA is not required?

- When the data processing operations are included in the list of data processing operations non requiring a DPIA compiled by the DPA
- When the personal data are processed in order to comply with a legal obligation or in the public interest, on the basis of EU law or the Member State's law, and an impact

[58] Article 29 Working Party (n 286) 9–11.
[59] ibid 11.

assessment essentially satisfying the conditions laid down in the GDPR has already been performed in the context of the adoption of that legal basis.

- When processing operations concern personal data from patients or clients by an individual physician, other health care professional or lawyer, because they are not considered to be on a large scale.

(g) How to conduct a DPIA?

The GDPR provides data controllers with flexibility to determine the precise structure and form of the DPIA in order to allow for this to fit with existing practices. National Data Protection Authorities may provide different methods and templates for carrying out the DPIA.

A proposed method for carrying on a DPIA, as interpreted from the GDPR, includes the following steps:

1) Make a screening (threshold analysis) of the processing operations in order to determine whether a process of DPIA is required
2) Provide a description of the envisaged processing operations, both contextual and technical, including, where applicable, the legitimate interest pursued by the controller and a diagram of data flows
3) Appraise the impact of the envisaged processing operation, in particular the necessity and proportionality of the processing operations in relation to their purposes, on the one hand; and the risks to the rights and freedoms of data subjects, on the other hand. The notion of risk refers to the data subjects, NOT to the SME.
4) Involve data subjects and/or their representatives, the data protection officer and any other expert (e.g. information security officer) and the data processor in the process, ideally in each phase of the assessment process.
5) Issue recommendations to address the identified risks and ensure compliance with the GDPR.
6) Activate a prior consultation procedure with a DPA in case the risks cannot be sufficiently mitigated, having regard to the recommendations that have been issued.
7) Perform a review, periodically or any time there is a change of the risk represented by processing operations. Carrying out a DPIA is a continual process, not a one-time exercise. A DPIA should be continuously reviewed and regularly re-assessed.

(h) When a new (revised) DPIA is required?

A new (i.e. revised version of) DPIA could be required if the risks resulting from the processing operations change, for example because **a new technology** has been introduced or because personal data is being used for a different purpose. Data processing operations can evolve quickly and **new vulnerabilities** can arise. Therefore, it should be noted that the **revision of a DPIA is** not only **useful for continuous improvement**, but also critical to maintain the level of data protection in a changing environment over time. A new DPIA may also become necessary because the **organisational or societal context for the processing activity has changed**, for example because the effects of certain automated decisions have become more significant, or **new categories of data subjects become vulnerable** to discrimination.

Each of these examples could be an element that leads to a change in the risk analysis concerning the processing activity at hand. Conversely, certain changes could lower the risk as well. For example, a processing operation could evolve so that decisions are no longer automated or if a monitoring activity is no longer systematic. In that case, the review of the risk analysis made can show that the performance of a DPIA is no longer required.

Important notice:

The mere fact that the conditions triggering the obligation to carry out DPIA have not been met does not diminish controllers' general obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects.

Best practices

In case of doubt concerning the performance of a DPIA, it is best practice to start the process.

Document every step (e.g. why the SME decided not to perform a DPIA, why the SME decided (not) to consult stakeholders in each phase of the process etc.).

Risks for non-compliance: infringement related to the performance of a Data Protection Impact Assessment can lead to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year.

6.3.10 Security requirements

(a) Background

Article 32 requires controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, such measures may include but are not limited to

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(b) How security obligation is related to other provisions?

This obligation also requires the controller to take due diligence and assess whether the guarantees offered by the processor, in this case the cloud service provider, are sufficient. During this process, the controller may take into account whether the processor provides adequate documentation proving compliance with data protection principles that could be found in privacy policies, records management policies, information security policies, external audit reports, certifications and similar documentation. The controller in particular should take into account the processor's expert knowledge (e.g. technical expertise when dealing with data breaches and security measures), reliability and its resources. After carrying out the due diligence process, the controller should be able to take a decision with sufficient evidence demonstrating that the processor is suitable, it can then enter into an arrangement. It should be added that this due

diligence process is not a one-time effort and it needs to be regularly repeated in order to check whether the processor is compliant. When outsourcing the processing of personal data (e.g. for the provision of technical assistance or cloud services), the controller should conclude a contract, another legal act or binding arrangement with the other entity already setting out clear and precise data protection obligations.

(c) What organizational security measures can SME take?

Carrying out an information risk assessment is one example of an organisational measure, but controllers and processors will need to take other measures as well. Each organisations should aim to build a culture of security awareness within your organisation.

An information security policy foreseeing the role of each user and permission levels (access control) appropriate to the role including the system administrator accounts is an example of an appropriate organisational measure.

(d) What technical security measures can SME take?

What technical measures do we need to consider?

Technical measures are sometimes thought of as the protection of personal data held in computers and networks. Whilst these are of obvious importance, many security incidents can be due to the theft or loss of equipment, the abandonment of old computers or hard-copy records being lost, stolen or incorrectly disposed of. Technical measures therefore include both physical and computer or IT security.

When considering physical security, you should look at factors such as:

- the quality of doors and locks, and the protection of your premises by such means as alarms, security lighting or CCTV;
- how you control access to your premises, and how visitors are supervised;
- how you dispose of any paper and electronic waste; and
- how you keep IT equipment, particularly mobile devices, secure.
- In the IT context, technical measures may sometimes be referred to as 'cybersecurity'. This is a complex technical area that is constantly evolving, with new threats and vulnerabilities always emerging. It may therefore be sensible to assume that your systems are vulnerable and take steps to protect them.

When considering cybersecurity, you should look at factors such as:

- system security – the security of your network and information systems, including those which process personal data;
- data security – the security of the data you hold within your systems, e.g., ensuring appropriate access controls are in place and that data is held securely;
- online security – e.g. the security of your website and any other online service or application that you use; and
- device security – including policies on Bring-your-own-Device (BYOD) if you offer it.

(e) What level of security is required?

The GDPR does not define the security measures that you should have in place. It requires controllers and processors to have a level of security that is 'appropriate' to the risks presented by your processing. Both controllers and processors need to consider this in relation to the state of the art and costs of implementation, as well as the nature, scope, context and purpose of the processing.

This reflects both the GDPR's risk-based approach, and that there is no 'one size fits all' solution to information security. It means that what's 'appropriate' for each controller and processor will

depend on their own circumstances, the processing they are engaged, and the risks it presents to their organization as well as the rights and freedoms of data subjects.

So, before deciding what measures are appropriate, you need to assess your information risk. You should review the personal data you hold and the way you use it in order to assess how valuable, sensitive or confidential it is – as well as the damage or distress that may be caused if the data was compromised. You should also take account of factors such as:

- the nature and extent of your organisation's premises and computer systems;
- the number of staff you have and the extent of their access to personal data; and
- any personal data held or used by a data processor acting on your behalf.

6.3.11 Personal data breach notification

(a) Background

Personal data breach notifications to DPAs and individuals accompanies a number of other provisions, such as data protection by design, security measures, data protection impact assessments and certification that also imbed *the risk-based approach.* As noted by European data protection regulators, a risk-based approach, while has been further articulated, is not a new addition to the EU data protection framework but rather an extension of the existing principles imbedded in the text of the Data Protection Directive, in particular, in the articles on the security (Article 17), the DPA prior checking obligations (Article 20) and the more stringent requirements for the processing of special categories of data (Article 8).[60] The notion of a risk-based approach in the GDPR is used in an attempt to update and modernise the EU data protection framework. The use of this notion allows to move from a legal compliance-based approach associated with provisions of the Data Protection Directive to 'a strong harm-based approach' focusing on 'responsible data use based on risk management'.[61]

According to the explanation provided by European data protection regulators, an obligation to notify personal data breach is both an accountability obligation and an obligation requiring 'additional measures when specific risks are identified'.[62] While being an accountability obligation a data breach notification is part of controllers' obligations, which 'can and should be varied according to the type of processing and the privacy risks for data subjects.'[63] An identification of risk of personal data breach in the data protection impact assessment would require controllers to put appropriate measures in place to 'treat risk' by modifying, mitigating, retaining, removing or sharing it.

(b) Under what conditions is a notification to the DPA required?

The GDPR requires that '[i]n the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority'.[64]

---

[60] Article 29 Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (2014) 2.
[61] ibid 3.
[62] ibid 3–4.
[63] ibid 3.
[64] European Union Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ EC (GDPR) Article 33.1.

To implement this obligation the controller must become aware about the personal data breach, which may include 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.[65] Consequently, this means that the controller must have an internal procedure allowing to confirm breach of security concerning personal data. The GDPR does not specify practical aspects of such procedure. At the same time, it is widely recognised that for any entity handling information, including processing personal data, to run in a smooth way it must have an appropriate governance or organizational structure in place where roles and responsibilities of individuals involved would be specified in internal policy and strategy documents. Such documents can be developed based on standards, guidelines and models provided by external sources yet it is essential that they consider relationships within the entity, its values and culture as well as its contractual relationships. Having this contextual awareness as well as awareness of data breach risk are incremental when developing an information incident response policy and plan, which can include obligations stemming from the GDPR as well as other regulatory frameworks (e.g., NIS Directive or the Payment services (PSD 2) Directive (EU) 2015/2366).

In an ideal scenario, an information incident response policy should precede the occurrence of an incident so that it could be used should a data breach take place.

(c) What documentation could help SME to prepare for a data breach?

The following documents in place that would assist in case of a (personal) data breach:

> '1) **Policy** is a high-level document outlining the goal and objective of the incident response program, the scope of the program across the organization, program roles, responsibilities, and authority and how program outputs such as incident communication and reporting will be managed.
>
> 2) **Plan** is a formal document outlining how the high-level policy document will be implemented and operationalized within the organization. Core elements of a security incident response plan include communication protocols that will be used to manage the sharing of incident updates and reports with internal and external stakeholders, metrics for measuring the effectiveness of the program, events that would trigger an update to the plan, and the strategy to improve and mature the plan over time.
>
> 3) **Standard Operating Procedures** are documents containing technical step-by-step actions that the CSIR Team will take to manage specific incidents. Standard Operating Procedures (SOPs) help minimize incident management errors and ensure a consistent and repeatable incident management capability. SOPs traditionally also include the forms and checklists that will be used by CSIR Team members in the execution of the CSIR Team.'[66]

(d) Under what conditions is a notification to affected individuals required?

The WP29 analysis does however establish clear threshold criteria when to notify individuals. The WP 29 points out that the high risk threshold for communicating a breach to individuals is higher than for notifying DPAs so that individuals are protected from 'unnecessary notification fatigue' and do not receive notification about all breaches.[67] In view of this, the WP29 suggests considering the following elements of the breach to determine if it entails high risks:

---

[65] ibid Article 4.12.
[66] Kevvie Fowler, *Data Breach Preparation and Response: Breaches Are Certain, Impact Is Not* (2016) Kindle edition 50.
[67] ibid.

- **The type of breach**: the WP 29 deems that the level of risk presented by data breaches depends if the breach concerns the principle of confidentiality, the principle of integrity and the principle of availability.[68] While to some extent this may be true, the guidance fails to recognise that data breaches typically have different motivations: they can be financially motivated cybercrimes, cyberespionage (concerning national security or economic interests), or acts aiming to publicly humiliate someone without an intention of attaining financial gains.[69]
- **The nature, sensitivity, and volume of personal data**: the risk evaluation largely depends on the sensitivity of personal data that was subject to a data breach. However, this sensitivity is often contextual (e.g., a name and address could be sensitivite if it concerns an adoptive parent), similarly to considerations concerning the volume of breached data. While typically the larger the volume of data is breached, the greater the impact may be anticipated, 'a small amount of highly sensitive personal data can have a high impact on an individual.'[70] It is also recognised that while data breaches concerning health data, identity documents and credit card details entail risks, the possibility to combine this data creates higher risk than a single piece of information, as it subsequently could facilitate an identity theft.[71]
- **Ease of identification of individuals**: when evaluating risks associated with a data breach, it is also important to consider for controllers whether identification of individuals who were subject to a breach is going to be easy. In this regard, the controllers should be asking if the compromised data can be matched with other data sets and what kind of security measures were implemented (e.g., what is the level of hashing, encryption or pseudonymization).
- **Severity of consequences for individuals**: the WP29 argues that controllers by taking into account the nature of the personal data involved in a breach (e.g., access to special categories of data, financial data) can anticipate the potential damage to individuals.
- **Special characteristics of the individual**: the controller when considering the impact on individuals needs to consider, example, if the breach concerns personal data about vulnerable individuals or individuals who due to some specific characteristics could be placed at greater risk of harm.
- **Special characteristics of the data controller**: the WP29 suggests that '[t]he nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach.'[72]
- **The number of affected individuals**: finally, the controller needs to weigh the amount of personal data that was compromised. In general, it is argued that large scale data breaches will have a more severe impact, however, as pointed out already, a personal data breach involving special categories of personal data of one person can have a severe impact as well.[73]

On the other hand, the test proposed by the WP29 to evaluate the risk that is likely to result from a breach is more finely defined and articulated. The test requires that each element is evaluated by the controller and that the decisions concerning notifications to DPAs and individuals are documented (i.e., to notify or not). The WP29 in its opinion regrettably avoids demonstrating how this test could play out in practice. Instead it introduces an analysis suggesting that the following personal data breaches scenario are of high risk to rights and freedoms of individuals: exfiltration of data entered to the website (i.e., a data breach situation in case of British Airways breach in

[68] ibid 7.
[69] Josephine Wolff, *You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches* (Kindle, MIT Press 2018) Location 2743 of 6938.
[70] Article 29 Data Protection Working Party, 'Guidelines on Personal Data Breach Notification under Regulation 2016/679' (n 207) 24.
[71] ibid.
[72] ibid 25.
[73] While in principle large scale data breaches will have a more severe impact, a personal data breach involving data of one person can have a severe impact as well.

September 2018), ransomware attack encrypting data, an unauthorised access to customer data breach, cyberattack against a hospital medical records database, sending an email with personal data to the wrong list of recipients, sending a direct marketing email revealing other recipients.[74] In this regard guidance provided by national data protection authorities may be of great interest. The Irish Data Protection Commission, for example, in its guidelines provides for more specific scenarios explaining when notifications concerning personal data breaches should be made by the controller.[75]

[74] Article 29 Data Protection Working Party, 'Guidelines on Personal Data Breach Notification under Regulation 2016/679' (n 207) 31–33.
[75] Irish Data Protection Commission, 'A Practical Guide to Personal Data Breach Notifications under the GDPR' (2019).

Glossary

Data controller: It is the natural or legal person which, alone or jointly with others (joint controllers), determines the purposes and means of the processing of personal data.

Data processor: means a natural or legal person which processes personal data on behalf of the controller; also in this case, factual circulstances prevail and the role may be assigned by Union or Member State law.

Data subject: an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Public authority or body: it is not defined in the GDPR, nor does the Regulation refer to national laws for the purpose of determining its meaning. Thus, the term should be given an autonomous EU- wide meaning. It encompasses those legal persons governed by public law or by private law, which are entrusted, under the legal regime applicable to them, with the performance of services of public interest and which are, for this purpose, vested with special powers beyond those which result from the normal rules applicable in relations between persons governed by private law. (see e.g. Case C- 279/ 12, Fish Legal and Shirley, para. 42 and case law cited therein).

Core activities: they are the key operations necessary to achieve the controller's or processor's goals. If the processing of data forms an inextricable part of the controller's or processor's activity, then it can be considered a core activity (e.g. if an SME carries out the surveillance of a number of private shopping centres and public spaces, surveillance is the core activity of the company, but it is at the same time inextricably linked to the processing of personal data).

Regular: meaning that it constantly or periodically taking place (i.e. ongoing or occurring at particular intervals for a particular period , or it is recurring or repeated at fixed times)

Systematic: meaning that it is occurring according to a system; pre-arranged, organised or methodical; taking place as part of a general plan for data collection; carried out as part of a strategy.

Monitoring: it happens when *natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes* (Recital 24 GDPR)

Large scale: there is a number of factors to consider in order to determining whether the processing is carried out on a large scale: the number of data subjects concerned (either as a specific number or as a proportion of the relevant population); the volume of data and/or the range of different data items being processed; the duration, or permanence, of the data processing activity; the geographical extent of the processing activity.

Exeptions to large scale: personal data should not be considered processed on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyers (Recital 91 GDPR).

Special categories of data: they are those personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms and for this reason they deserve specific protection. They are those data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (when processed for the purpose of uniquely identifying a natural person), data concerning health or data concerning a natural person's sex life or sexual orientation.

Exception to special categories of data: The processing of **photographs** should not systematically be considered to be processing of special categories of personal data! They are

covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person