HOMO DIGITALIS:

INPUT FOR

EUROPEAN COMMISSION 2024 REPORT ON THE APPLICATION OF THE GDPR

6 February 2024

This report was drafted by members of Homo Digitalis, as per the official questionnaire of the European Commission available here. Homo Digitalis has answered only questions in which it could provide meaningful input, based on its role and experience. The numbering follows the numbering of the official questionnaire.

A FEW WORDS ABOUT HOMO DIGITALIS

Homo Digitalis is the first civil society organization in Greece with the goal to protect and promote digital rights. We envisage a fair, open & transparent digital era, in which technology enables people's prosperity, proactively balancing progress with human rights respect.

Our mission is to raise awareness & protect digital rights and freedoms. We inform the public, we advise the decision-making bodies, and we intervene when the adequate level for their protection is not met. We are a team full of passion & energy, laying the grounds for digital rights to thrive in Greece and Europe.

1. General comments

a. What is your overall assessment (benefits/challenges, increase in trust and awareness, etc.) of the application of the GDPR since May 2018? Are there priority issues to be addressed?

Reflecting on the implementation of the General Data Protection Regulation (GDPR) since May 2018, our overall assessment is **positive**.

(i) The GDPR has undeniably served as a cornerstone in establishing strong guidelines for member states, setting a comprehensive framework for elevated data protection standards.

(ii) Over the course of its five-year tenure, GDPR has played a pivotal role not only in safeguarding individuals' privacy but also in cultivating a heightened awareness among citizens regarding their data protection rights. Data subjects are more aware of their rights and are increasingly exercising them, as evidenced by the gradual increase in the number of complaints filed with the Hellenic Data Protection Authority (HDPA) in case of violations.

(iii) In addition, private companies, acting as data controllers or data processors, have taken legal and technical measures to ensure the compliance with the GDPR and the implementing Greek Law No. 4624/2022;[1] and **(iv)** the number and amount of imposed penalties by HDPA have progressively increased since 2018.

However, within the successes, several **challenges** persist.

(i) One of the notable issues revolves around the diverse approaches taken by member states in implementing the GDPR. While the flexibility

[1] *There is no data available to show the number of companies that have adopted GDPR compliance measures.*

provided for specialization through national legislations can be beneficial, it simultaneously introduces a level of disparity that may impede the harmonization of data protection practices across the European Union. This calls for a more in-depth exploration to ensure a consistent application of the regulation, fostering a unified data protection landscape.

(ii) The effective management of data transfers and the promotion of collaboration among data protection authorities pose significant hurdles. These challenges need careful consideration to facilitate smoother cross-border data flow and enhance cooperation among entities responsible for enforcing the GDPR.

(iii) Many companies are still treating GDPR as a "checklist" obligation and have not actively adopted a data protection culture.

(iv) There are many challenges related to the delay by data controllers in fulfilling the rights of data subjects.

(v) The level of fines imposed by the HDPA is disproportionate to the size of certain companies, and the imposition of fines does not act as a deterrent. As a result, there is uncertainty as to whether the fines actually serve the purpose of preventing the recurrence of unlawful processing in the future.

(vi) Incomplete knowledge and abusive use of GDPR provisions by certain data processors and their employees have been used as a shield to conceal information. For example, representatives of public authorities and private companies have denied lawful access to personal data and even non-personal data (e.g. documents) because they wrongly perceive the access as unlawful; customer service representatives have refused to introduce themselves because they believe they are allowed to do so by virtue of the GDPR, leading to uncertainty in the customer service

experience; data controllers have not based the processing of special categories of personal data on Article 6 because they consider the sole application of Article 9 to be sufficient, whereas, correctly interpreted, any processing of special categories of data should be based on the combined application of Articles 6 and 9.

(vii) There is a lack of training services for technical compliance with the GDPR. The technical and organisational measures are very often poorly implemented, due to a lack of know-how and the absence of institutions that could provide training and practical guidance.

(viii) The recent "pay or okay" method used in consideration for the provision of digital services (e.g. for access and use of social media) has confused many data subjects about the extent to which they can control their personal data.

(ix) Lastly, an emerging concern revolves around the handling of Inferred Data, an aspect not explicitly addressed in the regulation's text. Inferred data refers to information that is deduced or derived from existing data through analysis, interpretation, or processing. It involves drawing conclusions, making assumptions, or predicting additional details based on the available information. This type of data is often generated through advanced analytics, machine learning algorithms, or artificial intelligence systems that can identify patterns and correlations within datasets, enabling the extraction of implicit information. This omission has created a significant gray zone for enterprises, as the lack of specific guidelines regarding inferred data has led to uncertainty in interpreting and implementing compliance measures. This ambiguity poses challenges in establishing clear boundaries for data processing practices, potentially allowing for unintended consequences and ethical concerns related to the

use of inferred data in the absence of explicit regulatory guidance. As technology continues to evolve, there is a growing need for regulatory frameworks to address these emerging challenges and provide clarity on the responsible use of inferred data within the context of data protection laws.

In conclusion, while celebrating the successes of the GDPR, it is essential to address these challenges. To ensure that the GDPR continues to evolve as an effective tool in safeguarding the privacy rights of individuals in the digital age there is need to harmonize national implementation, streamline data transfers, shorten the response time of companies by creating incentives for compliant companies (e.g. getting a tax reduction) and disincentives for non-compliant companies (e.g. automatic calculation of a fee in case no response is proven by the HDPA).

There is also need to shorten the response time of data protection authorities to issue a judgment; to impose higher penalties that can act as a deterrent and that are actually proportionate to the annual turnover of companies; to launch guidance tools to prevent misinterpretation and misuse of the GDPR (e.g. Q&A on the correct use of the GDPR); to support technical compliance; to clarify the picture on the lawful use of data by companies as a means of payment, rather than maintaining the vagueness on the nature of personal data, as the latter can be used against the interests of data subjects; and to provide clarity on Inferred Data.

Finally, given the ever increasing importance and potential of AI Technologies, the data protection risks associated with such technologies, the fact that one of the main tools to regulate the use of such technologies in the GDPR is Art.22, and the fact that until now Art.22 GDPR has been one of the most underused tools available to DPAs and Courts around the EU, the issuing of specific guidelines on the proper application of

Art.22 GDPR and its interaction with AI systems should be one of the highest priorities to ensure the protection of data subjects.

2. Exercise of data subject rights

a. From the individuals' perspective:

please provide information on the exercise of the data subject rights listed below, including on possible challenges (e.g. delays in controllers/processors reply, clarity of information, procedures for exercise of rights, restrictions on the basis of legislative measures, etc.).

• Information obligations, including the type and level of detail of the information to be provided (Articles 12 to 14)

• Access to data (Article 15)

• Rectification (Article 16)

• Erasure (Article 17)

• Data portability (Article 20)

• Right to object (Article 21)

• Meaningful explanation and human intervention in automated decision making (Article 22)

Where possible please provide a quantification and information on the evolution of the exercise of these rights since the entry into application of the GDPR.

Information Obligations (Articles 12 to 14): The right to information obligations empowers individuals to be informed about the processing of their personal data. However, challenges often arise in the form of unclear or convoluted privacy notices, causing confusion for data subjects. Delays in providing comprehensive information and insufficient detail regarding data processing practices can hinder the effectiveness of this right, necessitating clearer communication practices from data controllers and processors. For example, a common challenge may involve major contradicting provisions or minor typographical errors in privacy notices that might be overlooked, leading to inadvertent confusion. Additionally, the existence of dark patterns, deceptive design choices aiming to manipulate users, further complicates the exercise of this right. Considering these obstacles, it may be beneficial to use standard icons as an additional method to assist users in understanding the essence of the personal processing conducted.

Access to Data (Article 15): Article 15 grants individuals the right to confirm the processing of their personal data and obtain access to it. Challenges may emerge from delays in providing access, verification issues related to the identity of the data subject, or refusals based on legal grounds. In some instances, simple administrative errors, like misspelling a data subject's name, might lead to delays or verification hiccups, highlighting the need for meticulous data handling.

Rectification (Article 16): The right to rectification allows data subjects to request corrections to inaccurate personal data. Challenges may manifest in delays in processing rectification requests, disagreements over the accuracy of the data, or difficulties in implementing corrections. Organizations must establish efficient mechanisms to address and rectify inaccuracies promptly, fostering transparency and accuracy in their data processing practices. Occasionally, miscommunications within the organization might lead to delays, underlining the importance of streamlined internal processes.

Erasure (Article 17): Article 17 provides the right to erasure, enabling individuals to request the deletion of their personal data. Challenges can arise in disputes over the application of the right, legal obligations mandating data retention, or technical complexities in the deletion process. Instances where organizations face difficulty in clearly delineating between data that should be retained for legal purposes and data subject to erasure requests can introduce nuanced challenges.

Data Portability (Article 20): The right to data portability allows individuals to request their personal data in a portable and machine-readable format. Challenges may include technical limitations, difficulties in seamless data transfer to other service providers, or disputes regarding the applicability of this right. Organizations must ensure compatibility and interoperability to facilitate the smooth exercise of data portability rights, promoting user control over their information. Technical glitches, such as formatting issues in the transferred data, may arise, emphasizing the need for ongoing refinement in data portability processes. It must be noted that the right to data portability is often disregarded and scarcely exercised. Without guidelines and incentives, it is tranquilized.

Right to Object (Article 21): Article 21 grants individuals the right to object to the processing of their personal data. Challenges may involve disagreements over the legitimacy of data processing grounds, delays in responding to objections, or complexities in demonstrating compelling legitimate grounds. Human errors, like oversight in documenting legitimate grounds for processing, can introduce challenges in responding promptly to objections.

Meaningful Explanation and Human Intervention (Article 22): The right to meaningful explanation and human intervention in automated decision-making safeguards individuals from the potentially adverse effects of automated decisions.

Challenges may stem from insufficient explanations, difficulties in securing human intervention, or disputes over the legal implications of automated decisions. Minor communication lapses in providing meaningful explanations could contribute to challenges in the exercise of this right.

b. Do you avail of / are you aware of tools or user-friendly procedures to facilitate the exercise of data subject rights?

A user-friendly platform to facilitate the exercise of data subject rights is My Data Done Right Originally launched in the Netherlands by Bits of Freedom in 2018, this platform was introduced to Greece by Homo Digitalis on September 1, 2020. This platform aims to help users easily and quickly exercise some of the most important rights provided by the GDPR.

Specifically, through the platform, individuals can exercise rights such as access, deletion, correction, and data portability. Homo Digitalis has added over 150 organizations to the database in Greece, enabling users to utilize their contact information and expedite their requests. These organizations include contact details from banks, financial institutions, airlines, maritime companies, political parties, clothing and footwear companies, supermarkets, and more. (https://www.mydatadoneright.eu)

d. Are there any particular challenges in relation to the exercise of data subject rights by children?

In the digital age, issues such as obtaining informed consent from minors, ensuring privacy literacy, protecting against online bullying, and navigating parental control complexities pose significant challenges. Balancing children's rights to privacy with their participation in online activities raises concerns about age verification, transparency in data processing, and the potential impact of targeted marketing. Additionally, gaps in education about data rights for children further complicate their ability to navigate and assert these rights effectively. Addressing these challenges requires collaborative efforts from policymakers, educators, parents, and the technology industry to create a secure and empowering digital environment for children.

Specifically, the requirement for verified parental consent for individuals under the age of 16, as outlined in GDPR, adds a layer of complexity.

The implementation of the Self-Sovereign Identity (SSI) technology might provide for a great instrument in verifying the end users' age without revealing the rest of the end users' data. Homo Digitalis endorses the idea of wider research on the use of SSI and its adoption, firmly believing that it can solve may personal data issues, including enhancing the protection of minors.

Ensuring that minors comprehend the significance of data processing and have the capacity to provide informed consent is a persistent challenge. Moreover, children may not be fully aware of their rights as data subjects, emphasizing the need for enhanced education initiatives. Empowering children with knowledge about their data rights is crucial for fostering a culture of digital responsibility and enabling them to navigate the complexities of the digital landscape more effectively.

3. Application of the GDPR to SMEs

a. What are the lessons learned from the application of the GDPR to SMEs?

The application of the GDPR by SMEs seems to be one of the areas in which the application of the Regulation is not as successful as it could potentially be. This stems from three separate but interconnected phenomena:

(i) While the GDPR contains provisions for the scalability of the obligations and the application of the principle of proportionality, practical examples seem to indicate that the scalability of obligations is unbalanced in favor of bigger organizations, who have the ability and resources to achieve a minimum viable effort level of compliance with the Regulation without any impact in their day to day operations or business models -regardless of the risks that such operations may pose to the protection of personal data-, and in the detriment of SMEs who lack the ability and resources to achieve this minimum viable effort level of compliance without seriously impacting their operations, business model, or overall fiscal viability. This imbalance cannot be easily navigated by an SME by applying the principle of proportionality, since the de facto minimum compliance requirements are -by their nature- disproportionate for smaller SMEs.

(ii) The lack of an appropriate and dissuasive level of enforcement of the GDPR in many EU Jurisdictions, in combination with big delays in the inspection of cross border cases/complaints, and the bad faith practices of some data controllers which take advantage of the abovementioned phenomena, leads many SMEs to feel either that there is not sufficient incentive for them to properly apply the GDPR or that if they do decide to properly apply the rules

they are widening the gap with bigger competitors which do not properly apply the rules.

(iii) Even when SMEs decide to apply the rules, they often lack the resources and time to treat their compliance as anything more than a checkbox exercise.

In combination, these three phenomena lead to most SMEs either completely ignoring their obligations under the GDPR, or partially implementing them without developing a real culture of data protection within their organizations. Considering that a big percentage of EU enterprises are SMEs, this leads to a greatly reduced level of protection for personal data for all data subjects across the EU. Further guidance on the application of the rules, in combination with incentives for compliance for SME and an increase in the effectiveness and dissuasiveness of the application of the GDPR may lead to a considerable improvement in the level of compliance of SMEs.

b. Have the guidance and tools provided by data protection authorities and the EDPB in recent years assisted SMEs in their application of the GDPR (see also the EDPB data protection guide for small business)?

The Hellenic Data Protection Authority (HDPA) and the EDPB guidance and tools, such as the EDPB data protection guide for small business or the deliverables, guides, and templates of the "by design" project, which was completed by the HDPA, have assisted SMEs in their application of the GDPR. However, these tools are mostly used by SMEs which have already understood the value of GDPR compliance and have decided to dedicate some of their limited resources in complying with it. Additionally, many of the tools and guidance, when used by SMEs which have not yet developed a data protection culture and do not have access to expert advice, may further contribute

the misconception that GDPR compliance requires a checkbox approach and that it is enough for said SMEs to treat and use the guidance and tools as a plug and play solution, without actually implementing any other measures or understanding the rationale behind them.

In conclusion, guidance and tools have already greatly contributed to SME compliance and should be developed further. However, such tools are not enough –on their own- to solve all the issues which we identified in our answer to question 3.a.

4. Use of representative actions under Article 80 GDPR

b. For civil society organisations:

have you filed representative actions in any Member State (please specify: complaint to DPA or to court, claim for compensation; and the type of GDPR infringement) and if yes, what was your experience? Do you intend to take actions under the Representative Actions Directive?

Unfortunately, Homo Digitalis has not been able to file representative actions in Greece. The reason for this is that the Greek law (namely Law 4624/2019) did not provide that not-for-profit entities ('NPOs') have the right to lodge a complaint with the Greek Data Protection Authority and exercise the rights provided under GDPR articles 78-79, if it considers that the rights of a data subject under the GDPR have been infringed as a result of the processing, independently of a data subject's mandate.

Although the GDPR article 80, para 2 leaves absolute discretion in the Member States to decide if they will provide the above-mentioned option, the Greek legislator has decided to exclude this provision from the Greek law.

Homo Digitalis has underlined the importance of this provision since the early days of the public consultation for the Greek law – which was notably voted 15 months after 6 May 2018, when the deadline for adopting national legislation to implement GDPR provisions lapsed. By filing two memorandums and during a formal meeting with the law-drafting committee, as well as through one memorandum and a formal meeting with the Secretary General of the Ministry of Justice, Homo Digitalis had insisted on the significance of the adoption of this provision in the Greek law.

Civil society organizations, irrespective of their legal form, serve the public interest, democratic procedures and act as the intermediary between public authorities and the citizens. Their role is recognized under the Treaty of Functioning of the European Union article 15 and the United Nations Charter article 71.

The provision of GDPR article 80 para 2 provides an extra means of protections for the rights of individuals. While several major campaigns have been used to enhance the level of awareness of Greek citizens regarding their rights to their personal data, such level remains rather low. Therefore, there is a rather low level of exercising of said rights. By the Greek law providing the right to NPOs to exercise their rights only after being mandated by the data subject, we might face two important consequences:

(a) Data subjects may not become aware of a violation of the legislation, due to lack of information.
(b) Data subjects may be afraid to exercise their rights due to inequality of power (i.e. when the legislation is being violated by their employer or by a powerful third party).

Both cases shall result in non-exercising of their rights. Thus, the rights of individuals may severely be hampered. We sincerely hope that in future amendments to the Greek

legislation the right to file representative actions is provided to civil society organizations.

5. Experience with Data Protection Authorities (DPAs)

a. What is your experience in obtaining advice from DPAs?

Up to date the Hellenic Data Protection Authority has officially announced that it shall not be able to respond to requests regarding the implementation of the legislation, due to insufficient resources.

Homo Digitalis, since the early days of its establishment in March 2018 has highlighted the significance of providing Independent Authorities with sufficient human and economic resources to act. Independent Authorities constitute an important pillar for the protection of the rights of individuals and the enforcement of public scrutiny in modern democracies. Nonetheless, good intentions are not enough. For the Independent Authorities, including the HDPA, to successfully carry out their mission, resources are essential. The lack of resources for the HDPA since 2018 has been tremendous and has been highlighted in various occasions publicly by the HDPA itself and its members.

Insufficient resources for the HDPA remain an issue in 2024. Therefore, the HDPA still denies provision of advice to individuals, civil society organizations and private corporations. Notably, throughout the years, the HDPA has issued few Guidelines and Opinions, which are of excellent quality. Nonetheless, such Guidelines and Opinions are very few, while most of them have already become outdated – to note that the Opinion on the use of cameras dates back at 2011, when technology and implementation of cameras was totally different to today.

This situation enhances the gap between the legislation and its proper implementation with the individuals and entities in need lacking necessary guidance by the supervisory authority. It is essential that the HDPA is provided with adequate resources and that it drafts and implements a structured plan for the provision of advice to individuals and entities in need.

c. Are DPAs following up on each complaint submitted and providing information on the progress of the case?

Unfortunately, as already noted, the HDPA lacks resources. This results, among others, in a lack of information on the progress of cases, as well as provisions of statistics. It is worth mentioning that Homo Digitalis has filed 9 complaints before the HDPA so far, with only 1 decision taken and published hitherto – the one that imposed the largest fine in the history of the HDPA, 20 million euro to Clearview AI.

On an important note, one of the other 8 complaints filed by Homo Digitalis has been examined by the HDPA, a decision has been made since 21 December 2021. Nonetheless, the HDPA officials, when asked by Homo Digitalis, constantly state that the decision is since then –for 26 months now- in the process of "being typed". Neither Homo Digitalis nor the data subjects can have access to the decision until this process is completed.

6. Experience with accountability and the risk-based approach

a. What is your experience with the implementation of the principle of accountability?

The experience with implementing the principle of accountability in data protection has demonstrated varying degrees of success across organizations. Some have effectively embraced accountability, showcasing commitment through measures such as the development of comprehensive data protection policies, the conduct of Data Protection Impact Assessments (DPIAs), and the appointment of Data Protection Officers (DPOs) to oversee compliance. For instance, large enterprises with strong privacy frameworks often maintain detailed records of data processing activities, conduct regular audits, and proactively communicate their commitment to accountability.

However, challenges persist in the widespread adoption of accountability practices. Smaller organizations, constrained by limited resources, may struggle to establish and maintain sophisticated accountability frameworks. These challenges are highlighted by the difficulties faced in conducting thorough DPIAs, ensuring accurate record-keeping, and navigating the complexities of compliance requirements. In some cases, organizations may lack the awareness or expertise needed to effectively implement accountability measures, creating potential gaps in their data protection strategies.

Furthermore, it has often been observed that no audits are conducted regarding the DPO's appointment. Additionally, Data Protection Impact Assessments (DPIAs) are frequently perceived as extensive checklists without the inclusion of essential elements.

Instances of data incidents underline the critical need for more resilient accountability structures. Challenges include the need for continuous adaptation to evolving regulations, resource constraints hindering comprehensive compliance, and the

potential for inadequate awareness and understanding of accountability principles. Achieving a more consistent and effective implementation of the accountability principle requires ongoing efforts to address these challenges, enhance awareness, and provide support, particularly for smaller entities navigating the intricacies of data protection compliance.

b. What is your experience with the scalability of obligations (e.g., appropriate technical and organisational measures to ensure the security of processing, Data Protection Impact Assessment for high risks, etc.)?

The experience with the scalability of data protection obligations underscores the disparities between larger enterprises and smaller entities in effectively implementing these measures. Larger organizations, like Google and Microsoft, have demonstrated a more advanced capacity for scaling obligations, given their substantial financial and human resources that enable them to invest significantly in cutting-edge technologies, robust security infrastructure, and sophisticated encryption methods.

For instance, Google's implementation of advanced encryption standards across its services ensures a high level of security for user data, reflecting scalable measures aligned with data protection obligations. Notably, these large entities have the ability to hire specialized personnel or train their existing staff, ensuring a high level of expertise in implementing scalable measures aligned with data protection obligations.

In contrast, smaller entities, especially those with limited financial and human resources, encounter challenges in achieving similar scalability. Local businesses or startups may lack the means and specialized personnel to implement sophisticated technical measures and establish comprehensive organizational frameworks.

Conducting Data Protection Impact Assessments (DPIAs) for high-risk processing activities poses a notable challenge for smaller organizations, as they often face difficulties in navigating the complexities involved in assessing potential risks and implementing adequate safeguards.

Additionally, smaller entities often find themselves compelled to align with the practices of larger counterparts with whom they may collaborate. In collaborative partnerships or supply chain arrangements, smaller entities are frequently required to adhere to the established data protection standards of larger organizations.

This alignment, while necessary for seamless collaboration, can pose challenges for smaller entities that may lack the resources or technical capabilities to meet the same standards. The need for consistent adherence to the data protection obligations of larger entities may create hurdles for smaller organizations, highlighting the differences in their ability to independently scale and implement resilient measures.

The problem of inequality in resource allocation and technical capabilities is evident in the realm of data protection. Larger enterprises can play a crucial role in supporting smaller entities through collaborative initiatives. Regulatory bodies and industry associations can provide guidance, resources, and mentorship programs to facilitate the scaling of data protection obligations. By addressing the issue of inequality, the aim is to foster a collaborative environment where organizations of all sizes contribute to a uniform, comprehensive, and scalable implementation of data protection measures, promoting a secure digital landscape for all.

10. Have you experienced or observed any problems with the national legislation implementing the GDPR (e.g., divergences with the letter of GDPR, additional conditions, gold plating, etc.)?

At the very moment of the adoption of the National Law No. 4624/2019 implementing the GDPR (hereinafter 'Greek law'), the Hellenic Data Protection Authority identified several problematic points, which it highlighted in its Opinion No. 1/2020. The HDPA found that the Greek Law contradicts the GDPR on several occasions, and that the GDPR should always be given priority. In particular, it concluded that, in the exercise of its powers, it will not apply provisions of the Greek Law that are in contradiction with the GDPR or that are not based on clauses that allow for further specification. Two notable shortcomings of the Greek law are the following:

(i) While it follows from the provision of Article 10 GDPR that the national legislator is empowered to take the necessary measures by providing adequate safeguards for the processing of personal data relating to criminal convictions and offenses, the Greek Law does not take such measures, nor does the explanatory memorandum indicate the reason for this omission. Such measures have not yet been taken by the Greek legislator in any other sectoral legislation, which largely makes it impossible to apply the provision of Article 10 GDPR. (see HDPA opinion No 1/2020)

(ii) The Greek law does not provide that not-for-profit entities ('NPOs') have the right to lodge a complaint with the Greek Data Protection Authority and exercise the rights provided under GDPR articles 78-79, if it considers that the rights of a data subject under the GDPR have been infringed as a result of the processing, independently of a data subject's mandate. Although the GDPR article 80, para 2 leaves absolute discretion in the Member States to decide if they will provide the above-mentioned option, the Greek legislator has decided to exclude this provision from the Greek law. Thus, the

rights of individuals may severely be hampered. We sincerely hope that in future amendments to the Greek legislation the right to file representative actions is provided to civil society organizations. (see point **4 a.** for more information)

14. GDPR and innovation / new technologies

a. What is the overall impact of the GDPR on the approach to innovation and to new technologies?

GDPR's overall impact on the approach to innovation and new technologies proved to be both influential and positive for the protection of personal data. The obligations of the GDPR are acting as one of the cornerstones for the use of technologies and software which involve personal data. Additionally, the provisions of the GDPR have already been successfully used to protect the rights of data subjects from new technologies and innovative models which, while clearly incorporating features which violated the rights of the data subjects, were not yet specifically regulated at the time of their implementation due to their novelty.

However, it shall be noted that there have been many instances where the GDPR has been completely ignored during the development and implementation of new and innovative technologies by big market players/data controllers. In some of those instances the final product was launched and was widely used by the public without the appropriate data protection safeguards in place, proving that stricter enforcement may be needed to dissuade controllers from not protecting the rights of data subjects, especially when developing potentially high value/ high return technologies.

b. Please provide your views on the interaction between the GDPR and new initiatives under the Data Strategy (e.g., Data Act, Data Governance Act, European Health Data Space etc.)

The GDPR's impact in the application of the new initiatives will be important and we salute the overall goals which the Data Strategy attempts to achieve. However, the ever-increasing amount of new initiatives may create inconsistencies or confusion regarding the proper application of –potentially- conflicting provisions in specific scenarios. Currently, GDPR's interaction with the rest of the initiatives seems to be clear, but we believe that the future introduction of guidelines on the interplay between the GDPR and some specific provisions of said initiatives would provide greater certainty to data controllers and processors, reduce regulatory fatigue, and in general contribute to a higher and more consistent level of protection for data subjects.

Taking into consideration the increased importance and potential of AI technologies, we would like to comment specifically on some aspects of the interaction between the GDPR and the AI Act. It is clear that the provisions of the AI Act should be without prejudice to data protection law (recital 5 a of the AI Act), but also that data protection (achieved by the GDPR) should continue to ensure the promotion of innovation, the latter being a strategic objective of the Union.

Nevertheless, some specific areas of tension are the following:

(ii) The need to collect data for the training of AI systems may conflict with the fundamental principle of data minimisation (5§1 c GDPR). The training of systems requires the collection of personal data, which must be of high quality and essential for the structure and performance of AI systems, in particular the absence of discrimination prohibited by Union law (recital 44, AI Act). The mitigation of this controversy could be achieved through the operation of the regulatory sandboxes.

(iii) The need to collect data to prevent discrimination (which could result from a limited sample of data), as well as the need to collect large amounts of data to experiment with the capabilities of AI systems, may conflict with the basic purpose limitation principle (5§1 b GDPR). This principle prohibits the mass collection of personal data, and emphasises the need to define a specific lawful ground for processing in advance. The mitigation of this controversy could be achieved through the operation of the regulatory sandboxes.

(iv) There may be conflicts arising from the way AI systems are developed, trained and deployed with the remaining principles relating to the processing of personal data, such as the difficulty of ensuring the requirements of lawfulness, fairness and transparency (5§1 a GDPR), accuracy (5§1 d GDPR) and ensuring the accountability of the controller (5§2 GDPR).