Digital Omnibus

First Analysis of Select GDPR and ePrivacy Proposals by the Commission

Version 1.0

noyb.eu

Introduction

We have worked tirelessly on the Digital Omnibus over the past weeks, trying to conduct a deep analysis of all relevant changes. This is still early days, but certain problems, inconsistencies, or at least clear departure from the current logic of the GDPR or CJEU case law are evident.

There also seems to be a tendency that planned changes in the Digital Omnibus (e.g. rules on "consent banners") are somewhat mature, even if improvements to the texts seem warranted.

At the same time, many of the surprising last-minute changes, some of which were not even included in previously leaked inter service documents, seem to lack the legal quality to move ahead and may even provide more complication – not simplification for SMEs.

Given that this is a developing legal debate, we are very happy to receive your feedback at info@noyb.eu on errors in our report, but also for elements we have not (yet) identified and which we can add to the next versions of this report.

We plan to update the first version of this report with specific recommendations in the coming weeks. You will be able to find the latest version of this report at https://noyb.eu/en/reports-resources.

Thank you for your interest!

Max Schrems
Chairperson, *noyb*.eu

Table of Contents

Article 4(1) – Definition of "Personal Data"

Current Text

(1) 'personal data' means any information relating to an identified or identifiable natural person ('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;

Proposed Text

(1) 'personal data' means any information relating to an identified or identifiable natural person ('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. **Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.**

Current Relevant Recitals

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which

Proposed Recital

(27) This Regulation proposes a series of targeted amendments to Regulation (EU) 2016/679 for clarification and simplification, whilst preserving the same level of data protection. Article 4 of Regulation (EU) 2016/679 provides that personal data is any information relating to an identified or identifiable natural person. In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. Taking into account the case-law of the Court of Justice of the European Union concerning the definition of personal data, it is necessary to provide further clarity on when a natural person should be considered to be identifiable. The existence of additional information enabling the data subject to be identified does not, in itself, mean that pseudonymised data must be regarded as constituting, in all cases and for every person or entity, personal data for the purposes of the application of Regulation (EU) 2016/679. In

does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

particular, it should be clarified that information is not to be considered personal data for a given entity where that entity does not have means reasonably likely to be used to identify the natural person to whom the information relates. A potential subsequent transmission of that information to third parties who have means reasonably allowing them to identify the natural person to whom the information relates, such as cross-checking with other data at their disposal, renders that information personal data only for those third parties who have such means at their disposal. An entity for which the information is not personal data, in principle, does not fall within the scope of application of Regulation (EU) 2016/679. In this respect the Court of Justice of the European Union has held that a means of identifying the data subject is not reasonably likely to be used where the risk of identification appears in reality to be insignificant, in that the identification of that data subject is prohibited by law or impossible in practice, for example because it would involve a disproportionate effort in terms of time, cost and labour. An example of a prohibition against reidentification can be found in the obligations of health data users in Article 61(3) of Regulation (EU) 2025/327 of the European Parliament and of the Council35. The Commission, together with the European Data Protection Board, should support controllers in the application of this updated definition by stipulating technical criteria in an implementing act.

Overview

The Commission's proposal is meant to introduce a "subjective" approach to the definition of "personal data". It seems the idea is to exclude certain "pseudonymised" data (see Article 4(5) GDPR) from the scope of the GDPR – contrary to the current understanding that they are covered by the GDPR.

This would mean that data will increasingly be "personal" for *some* controllers – but not for others. Meaning that some would be covered by the GDPR and others not. Given that this is the core definition of the GDPR, it leads to massive consequences (e.g. on cooperation between controllers and processors, international data transfers, security requirements under Article 32 GDPR, availability of data subjects' rights and protections). Changes to the core definition would also have to be in line with the understanding of "personal data" in Article 8 of the Charter.

A key intellectual flaw of the definition seems to be that it is solely based on the role of the controller and the knowledge available to said controller – while B2B business partners, data subjects, and supervisory authorities lack any access to the relevant information that would allow the determination if any data is indeed sufficiently linked to a person. There is also a "chicken and egg" issue, because a claim of a controller that data is not covered by the GDPR would also call the right to access under Article 15 GDPR and the powers of supervisory authorities into question.

In combination with already weak enforcement and low GDPR compliance, this change would create not only another massive loophole for rogue actors to reject GDPR rights but also legal uncertainty for all

affected entities. Moreover, it would regularly fully frustrate or at least massively delay enforcement by supervisory authorities.

In Article 41a (see details below) the Commission further proposes that it can define by an implementing act what does not constitute "personal data" anymore, because pseudonymisation techniques were sufficient. This would indirectly give the Commission a major role in excluding entire industry sectors from the GDPR.

Charter

The definition of "*personal data*" in Article 8 of the Charter refers to the definition in Dir. 95/46 (see explanatory note of the Convention on the Charter). This sets a minimum standard.

Consequently, the European legislator has no powers to change the definition of "*personal data*" to encompass less than the understanding of Directive 95/46.

While the GDPR was supposed to have a slightly broader scope that went beyond Directive 95/46 (adding "*name*", "*location data*" and "*online identifier*"), the proposed definition in combination with the proposed Article 41a that seem to target "*pseudonyms*" would likely reduce the scope of application l below Directive 95/46:

- The wording of Article 2(a) of Directive 95/46 clearly states that "*identification numbers*" (which usually constitute "*pseudonyms*") were covered by Directive 95/46 and hence Article 8 of the Charter.
- It is therefore clear that any definition that excludes "*pseudonyms*" would in many cases get the GDPR into conflict with the Charter and hence create more legal instability compared to the current (well-established) understanding.

While the legislator has the option to roll back the definition to the scope covered by Directive 95/46, there seems to be very little room to exempt "*pseudonyms*" from the GDPR.

Case Law

There are numerous cases by the CJEU on the definition of "*personal data*", but the proposed draft relies solely on a selective interpretation of C-413/23P EDPS v SRB. This ruling had a a very specific fact pattern, but even the SRB decision seems to conflict with the proposed changes:

- In the SRB case (see § 24 of the ruling) IDs were given to comments (not people) and duplicate comments were merged under the same ID. Any resulting pair of ID and comment could have been from one or more persons, which is a very different pattern than "pseudonyms" where any ID corresponds to one person.
- The CJEU highlighted multiple times in the ruling that this case was about the question if the EDPS was correct that a "*pseudonym*" was "*in any case*" personal data (see §§ 68, 73, 80, 82 and 86). The case was sent back for further investigations. This does not allow to assume that the opposite is true in most cases.
- The CJEU highlighted that "*it is settled case-law that (…) it is not required that all the information enabling the identification of the data subject must be in the hands of one person*" (§ 99) and that data can be "*by reason of its content, purpose or effect, it is linked to an identifiable person*" (§ 55).
- The CJEU emphasised the "*broad interpretation*" (§ 54) of the concept of personal data and the need for a case-by-case analysis (§100), making the ruling a questionable basis to justify changes to a general law.

In summary, it is clear that the proposed changes in the draft go beyond the intention and ruling of the CJEU in SRB.

In the interest of a balanced and fair review of case law, the following rulings should have been taken into account – if the Commission would have actually intended to clarify the case law:

- C-582/14 *Breyer* – Dynamic IP addresses can be personal data, if there is a legal means to obtain additional information. In Breyer it was irrelevant if this is likely to be used, the possibility was sufficient (§48). This is at odds

with the proposed wording ("*means reasonably likely to be used by that entity*").

- C-434/16 *Nowak* – Data is personal data, even when there is no ID or name relating to that person for the examiner, but the processing of data still has consequences for a person (here: an exam, without a name or ID on the cover that was failed). The element of consequences (which are regularly the case if a person is identified via a pseudonym) is missing in the Commission draft.
- C-683/21 *Nacionalinis visuomenės sveikatos centras* holds that personal data which could be attributed to a natural person by the use of additional information must be considered to be information on an identifiable natural person (see § 58) – again, there is no indication that the subjective intention or "*likeliness*" of such a step plays any role.
- C-579/21 *Pankki* – Here the Court held that the expression '*any information*' mentioned in the definition of 'personal data' is to be interpreted to reflect an aim for the legislators to assign a wide scope to that concept (§42).
- C-604/22 *IAB Europe* – A string containing the preferences of a user is personal data (§43) and "*the mere fact that IAB Europe cannot itself combine the TC String with the IP address of a user's device and does not have the possibility of directly accessing the data processed by its members in the context of the TCF*" does not lead to the conclusion that it does not constitute "personal data" (§46). Even if the IAB clearly had no interest in "tracking" individuals" itself or was "*likely*" to do so, data still constituted "*personal data*". This is directly contrary to the proposed draft, that places weight on the subjective intentions of any individual controller.
- C-479/22 P *OC* – The court held that the if additional information were available to recipients of the information (here: the public) the information falls under the GDPR, already for the first controller (see § 64), which is clearly in direct conflict with the wording in the proposal ("*Such information does not become personal for that entity merely because a subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.*")

We note that the overall CJEU case law points in a very different direction than the changes intended by the Commission's proposal. . This further indicates that the insertion of highly subjective dimensions to the defintion of personal data under the GDPR could be seen as a violation of the Charter by the CJEU.

Legal Certainty

Generally, laws try to use objective factors for definitions, to ensure that laws do not have different meanings for different people.

Furthermore, to ensure legal certainty, ideally factors are chosen that are easy to assess for everyone that has interests in the matter or have to enforce them (see e.g. "*Publizitätsprinzip*", "principle of public disclosure" in civil law).

Making the application of laws dependent on largely internal, subjective decisions or abilities of *one* party leads to massive legal uncertainty for everyone else (data subjects, business partners or superiority authorities) and obviously allows simple manipulation.

Legal certainty can be challenged by underclaiming and overclaiming of GDPR application:

- If a controller falsely claims that the GDPR is not appliable when it is, this may have obvious consequences of fines or lawsuits for non-compliance with GDPR duties.
- However, also a false claim that data is protected by the GDPR may generate false trust with data subjects of business partners.

A major problem also seems to be the temporal aspects, what may not be likely today can become likely tomorrow – especially with fast developing technologies.

Overall, the addition does not improve legal certainty, but instead creates more confusion and need for clarifications by the CJEU.

Legal Quality

The wording of the new provision is highly unclear and prone to further confusion:

Of the three sentences added, only the second sentence seems to be an operational legal provision, while the first and third sentence are rather speculative:

- If data is "*not necessarily*" or not "*merely*" personal data because another person can identify it, the provision adds little to no clarification, as it neither says that such situations fall under Article 4(1) nor that they do not. Authorities, data subjects, or business partners may still claim that in any specific case because a recipient *can* identify the data.
- Even the second sentence opens major uncertainty, as it requires an assessment of the "*likeliness*" of each individual controller ("*that entity*") to use certain "*means*" to identity a person. This could be understood that the capabilities and even the ethics or trustworthiness of a controller or an industry sector would play a role in determining if they fall under the GDPR.

In practice this could lead to questions like:

- Would a small company do this? No, not able.
- Would a Bank do that? No, ethical limitations.
- Would Google do this? Maybe, but their privacy policy says no.
- Could Google do this in the future? Yes.
- Would a hacker do this? Sure.

Having the "core" definition that decides about the application of a law (with massive consequences for data subjects, but also controllers that can face a €20 million penalty) hinge on such unclear wording seems to be highly problematic from a rule of law perspective.

Conflicts

There seems to be increasing conflicts within the various definitions and recitals, that may lead to more confusion:

- Art 8 CFR, referring to Dir. 95/46 and forming "treaty law" have the reference to an "identification number", which would describe most pseudonyms. The definition does not clearly state that it is subjective, but generally follows an objective wording. The CJEU took a different view here.
- Recital 26 of the GDPR would typically include pseudonyms to the extent that they are assigned to a person (see "*singling out*").
- Recital 25 of the Omnibus seems to point at an even more lenient approach than the proposed additional elements in Article 4(1).
- The proposed amendment is in turn conflicting with the CJEU interpretation of Article 4(1) GDPR, that does in fact see mere consequences on a person (see C-434/16 *Nowak*) or the option of any recipient to identify the person (see C-479/22 P *OC*).

There are also logical conflicts with the structure of the GDPR:

- There is an inherent logical conflict as the (proper) separation of data and keys turn "*personal data*" into "*pseudonymous data*", however if a controller does not fall under *any* of the rules of the GDPR exactly the very rules that govern such proper separation (e.g. Article 32) would not apply anymore.
- It is unclear to what extent a controller can share data with another controller anymore that falls outside of the GDPR. This would create an obvious "data leak" an may conflict with Article 32 GDPR.
- It is unclear how joint controllerships would work if one of the controllers falls under the GDPR and others do not (see for example Plugins as in C-40/17 *Fashion ID*).
- It is unclear how this change in rules would impact the role of a processor, especially if a processor may engage in secondary use of personal data, but would itself not be able to identify an individual beyond pseudonyms. The current solution in Article 28(10) would not apply anymore.
- Equally the current system for international data transfers under Chapter V of the GDPR would fail to work if a "data exporter" that is unable to identify an individual would be put between an EU/EEA controller and a non-EU/EEA controller.

Overall, it seems that the change at the core definition of "personal data" could have massive unintended consequences throughout the GDPR that would need more research.

Simplification

For the broad mass of controllers this change would likely not lead to any material simplification, as most controllers will be unable to use pseudonymisation in any meaningful way.

In many cases the fact that the same data can switch several times between being covered and not covered may make management of GDPR compliance even more complicated.

For data subjects and supervisory authorities an increasing uncertainty if processing (on an opaque IT system) even falls under the GDPR would make the management of GDPR rights extremely complex.

Data Subjects

For data subjects any subjective definition holds massive problems:

- Data subjects would be inherently at the mercy of controllers to admit that a system holds "personal data", as they usually have no realistic path towards proofing the opposite.
- Any dispute about data being "personal data" would also exclude the exercise of the right to access under Article 15 GDPR, creating a "chicken and egg" problem.
- This could create years of litigation and even more complaints following access requests, that would need deep investigations into technical setups by supervisory authorities.
- Problematic controllers already use "any trick in the book" to reject GDPR rights, the subjective definition would generate an entire new toolbox of reasons to reject GDPR rights in practice.
- The fact that some supervisory authorities (e.g. in France, Germany, Sweden or the Netherland) only investigate complaints that have a "systematic" relevance, would mean that unlawfully rejected GDPR rights would have basically no realistic remedy. In most Member States a civil lawsuit costs €20,000 and more – especially if technical witnesses must be called in to determine the technical setup of a "pseudonymisation" technique.
- Even if data subjects ultimately win such battles, they take years and make the exercise of rights *de facto* worthless.

Overall, the prosed "subjective" approach risks to be the final nail in the coffin of GDPR rights, when it comes to the real-life enforcement of GDPR rights for data subjects.

Controllers

The consequences for controllers and processors may depend on the individual situation of a company. For normal small or medium size controllers this change may generate more complexity and uncertainty:

- While for individual controllers the provision would get more complex, it may be manageable, as they should have all relevant information before them.
- However, they would also have to assess any "*likeliness*" to (not) use certain "*means*" to a regulator and provide proof of that. If an SA would take a different view, the penalties of €20 million or 4% would be triggered.
- False statements that indicate that the GDPR would cover processing (when in fact it does not) could also trigger liability towards consumers.
- It is unclear if a controller could "opt into" the GDPR if the controller is not sure about the interpretation of Article 4(1) in a given case or if this result could be derived somehow (e.g. via the "*fairness*" principle).

Controllers that need to work with other controllers or processors may have more massive problems if a definition becomes even more subjective:

- Fights about the controller, joint controller or processor roles are a notorious ground for disputes in B2B relationships. An increasingly subjective definition would probably add to the (existing) problem.
- The cooperation between controllers could be massively limited if some controllers are not covered by the GDPR. The "covered" controller would expose personal data to a third-party that is outside of the protection of the GDPR. This could lead to massive security issues, because (other than truly anonymous

data) such data could be re-identified, for example by a third controller.

There may be benefits for large controllers that could "bypass" the GDPR by introducing sophisticated pseudonymisation schemes or technical approaches. However, the benefit to the digital market and society seems questionable.

Overall, it is highly likely that most controllers would face a more complex and uncertain legal situation, while a small number of (aggressive or highly sophisticated) controllers may find ways to fully escape the GDPR.

Supervisory Authorities

Given that the application of any provision in the GDPR hinges on the definition of "personal data", supervisory authorities would in many cases have to engage in extensive technical investigations to proof that they are even competent if such a a "subjective" approach is followed.

Controllers could easily derail investigations by simply claiming to not fall under the GDPR, which would easily prolong investigations for months and years – even if the argument is ultimately rejected. In many cases authorities may also "give up" if such an argument is brought, as it would require intensive technical investigations to disproof such a claim.

The subjective approach would mean massive additional work for authorities, at a time where most are already underfunded and unable to deal with their workloads.

Real Life Examples

Controllers regularly use any trick in the book to delay access request or other GDPR rights. Some examples from *noyb*'s experience:

- GDPR rights: *noyb*'s internal estimate is that at best 10% of all access requests are answered fully and within the legal deadline. User rights are more often not granted than granted. Currently less than 1.3% of all GDPR complaints lead to a fine. While many "honest" controllers do their best to comply, problematic controllers already use loopholes to bypass the GDPR. The subjective approach to Article 4(1) would massively increase such options.
- YouTube: It took *noyb* 5 ½ years to get access to the data in a YouTube account. Of 8 complaints none of the tested streaming companies fully complied with Article 15.
- Telco Tracking: The Austrian Data Protection Authority rejected access to phone network tracking data (location of a smart phone) because the phone data is not "personal data" as the phone could have been used by another person – even when the data subject has a fingerprint lock on the phone and filed an affidavit that he never shared the phone.

The matter if personal data is actually covered by the GDPR is already excessively argued by controllers. Some examples from noyb's experience:

- Microsoft Xandr: Microsoft's online tracking subsidiary Xandr responded to 0% of all requests under Article 15 GDPR, claiming that all of their online tracking would be "anonymous" even when Online Identifiers are explicitly mentioned in Article 4(1) GDPR.
- Online Tracking: In a recent court case against the Austrian page DerStandard, the controller argues that all the data flowing to hundreds or advertisement partners would not be "personal data", because DerStandard is allegedly unable to identify people based on shared IDs.
- Grindr: Many apps include "SDKs" in their software of third parties, that track users, without the main app being able to control the data or identify people. Grindr (a gay hookup app) used an SDK by Twitter's mopub that forwarded IDs to more than 4,259 partners. All relevant tracking was solely done based on location and random IDs, but can have very real life consequences for people (e.g. if such data is shared with governments that punish gay people).

Increasingly typical points in a customer journey where "hard" personal data was collected is outsourced, enabling controllers to argue that the remaining data is "pseudonymous":

- Login with Google/Facebook: Websites and apps increasingly outsource the user management to other companies, like Google or Facebook (seen by users as "Login with…"). This means that these websites may only store a random UUID anymore for users. This would still be covered under "*identification number*" in Article 4(1) GDPR, but would also be a "*pseudonym*". It is unclear if such an ID would still fall under the new Article 4(1).
- Payment: Increasingly payment is done via third parties (Stripe, Google Pay, Apple Pay) meaning that an app can have a subscription service without ever collecting name or billing address.

Article 4(38) - "Scientific Research"

Current Text

Proposed Text

(38) "scientific research" means any research which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial interest.

Current Relevant Recitals

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

(159) Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.

Proposed Recitals

(28) In order to assess whether research meets the conditions of scientific research for the purpose of this Regulation, account can be taken of elements such as methodological and systematic approach applied while conducting the research in the specific area. Research and technology development should be conducted in academic, industry and other settings, including small and medium-sized undertakings, (Article 179(2) TFEU) and should be always of a of high quality and should adhere to the principles of principles of reliability, honesty, respect and accountability (verifiability).

(29) It should be reiterated that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. In such cases it is not necessary to ascertain on the basis of Article 6(4) of this Regulation whether the purpose of the further processing is compatible with the purpose for which the personal data are initially collected.

(32) The processing of personal data for scientific research purposes and the application of the GDPR's provisions on scientific research are conditional on the adoption of appropriate safeguards for the rights and freedoms of data subjects, pursuant to Article 89(1) GDPR. To that end, the GDPR balances the right to protection of personal data, pursuant to Article 8 CFREU, with the freedom of science, pursuant to Article 13 CFREU. The processing of personal data for the

	purpose of scientific research therefore pursues a legitimate interest within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, provided that such research is not contrary to Union or Member State law. This is without prejudice to the obligation of the controller to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.

Overview

The GDPR currently refers to "scientific research" in Articles 5(1)(b) and (e), 9(2)(j), 14(5)(b), 17(3)(d), 21(6) and 89. So far this term was not legally defined in the text of the GDPR. However, the current definition of scientific research can be found in the non-binding Recital 159 of the GDPR: "*scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research*".

The EU Commission now proposes a new, extremely broad, definition of "*scientific research*" to be included in the GDPR, which would affect all the aforementioned provisions in the GDPR – which largely lead to an exemption from GDPR rights and duties.

The definition of "any research which can also support innovation" meaning that just the possibility ("can") of any byproduct ("also") that can help ("support") with an undefined notion of "*innovation*" (a claim that lately even "AI toothbrushes" would claim for themselves) would largely overcome limitations that derive from Article 8 of the Charter, like purpose limitation or data minimisation.

Limitations of the definition, such as the "*growth of society´s general knowledge and wellbeing*" have little legally enforceable meaning. Equally, the wording "*adhere to ethical standards in the relevant research area*" seem to be largely useless, given that many areas of commercial research either do not have agreed and enforceable enthical standards, or because such standards are drafted by the industry itself – leading to an outsourcing of limitation of decisions on a fundamental right in Article 8 of the Charter to private ethics standards.

In an Opinion of 6.1.2020 the EDPS, for defined research as follows: "*Scientific research applies the 'scientific method' of observing phenomena, formulating and testing a hypothesis for those phenomena, and concluding as to the validity of the hypothesis.*"

In Guidelines 03/2020 the European Data Protection Board followed the Article 29 WP259 and highlighted: "*the notion may not be stretched beyond its common meaning and understands that 'scientific research' in this context means a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice.*"

Charter

The purpose limitation principle and the need to have a legal basis are elements of Article 8(2) of the Charter. Equally, data minimisation is a logical consequence of Article 8 and the "*necessity*" requirement in Article 52(1) of the Charter. All of them are implemented in Article 5(1) GDPR. The right to deletion is the logical consequence of a lack of a legal basis under Article 8(2) of the Charter.

Hence, many of the "*research*" exemptions directly overturn rights that are protected by the Charter and would have to be "*necessary and proportionate*" under Article 52(1) of the Charter.

While it is undisputed that scientific research (a

"*freedom*" in Article 13 of the Charter) is a public interest that may allow limitations of other fundamental rights, any blanket allowance of further processing for a broadly and ill defined "*research purpose*" likely runs afoul the Charter - especially as the Commission does not seem to have done any relevant impact assessment.

Case Law

We were unable to find CJEU case law on Article 89 GDPR or the current understanding of "scientific research" in the GDPR.

In C-66/18 *Commission v Hungary*, the CJEU has in paragraph 225 to 228 given a short background of the understanding of "*scientific research*" as a freedom that derives from the right to free speech, to disseminate information and conduct research. Despite a "broad" definition, there is no indication that the proposed understating in Article 4(38) GDPR would be in line with Article 13 of the Charter.

At the same time, there are countless cases where any broad, unbalanced and absolute limitation of Article 7 and/or 8 of the Charter, be it for anything between transparency (see C-465/00 *ORF*) all the way to terrorist prevention (see C-293/12 - *Digital Rights Ireland*), is never in line with the Charter.

We therefore consider that the proposed broad definition, in combination with the direct waiver of Charter rights would probably not comply with CJEU case law.

Legal Quality

As with other definitions in the proposal, Article 4(38) has more than 20 (!) criteria, that are not always logical and partly contradict each other.

The first sentence contains a number of conditions that seem extremely vague and even contradictory to the general understanding of "scientific research":

- The definition uses core term "*research*", which is so broad that it covers sifting through a library, using Google Search or watching rats in a laboratory.
- This core term is broadened further by adding that "*any research*" is covered which "*can also*" support innovation. Which includes mere possibilities ("*can*") and mere byproducts ("*also*").
- On the other hand, any "*scientific research*" must be able to support innovation. This implies that academic research that is not aimed at "*innovation*" would be excluded from the new definition.
- The "*such as*" element is merely demonstrative but underscores that the definition tilts towards "*technical development and demonstration*" but not research in medicine, humanities or natural science.

Overall, the proposed core definition seems to fundamentally devalue the work of the scientific community for political gains in the name of "*innovation*".

Article 4(38) as proposed furthermore includes the following additional elements that make the definition finally almost unlimited:

- The element that merely "*apply[ing] existing knowledge in novel ways*" would constitute "*scientific research*" fully undermines the distinction between research and application. Applying an old legal argument in "*novel ways*" would already fall under this wording.
- The definition states that scientific research must have the "*aim of contributing to the growth of society´s general knowledge and wellbeing*", but this would include any economic processing operation that generates profits and thereby increases the economic "*wellbeing*" of society or merely makes information accessible (like Google Search or an AI bot).
- Finally, the reference to "*ethical standards*" may often fail as there are simply no agreed ethical standard in certain industry sectors (e.g. AI) and if such standards exist, they are typically drafted by the relevant industry or research sector itself. This generally leads to an "outsourcing" of rules about the Fundamental Right to Data Protection in Article 8 of the Charter to private actors, which is a clear violation of Article 52(1), that requires that limitations and any protections must be set out by "*law*".

In summary, these elements are not helping to clarify the exemption in any reasonable way, but add more confusion.

Conflicts

So far, the European legislator privileged research, but did not issue a *carte blanche*.

The definition and the broad exemption from Articles 5(1)(b) and (e), 9(2)(j), 14(5)(b), 17(3)(d) and 21(6) GDPR seem to be at odds with the system of Article 89(1) and (2) GDPR that requires "*appropriate safeguards*" for the rights and freedoms of data subjects. Article 89(1) and (2) therefore requires that Member States legislate in that area to balance interests.

The new definition likely conflicts with the various national definitions of "*scientific research*" that Member States passed to implement Article 89 GDPR and "*the common meaning*" of scientific research as addressed in the Article 29 WP259 in 2018.

For the likely conflicts with Articles 8 and 13 of the Charter see above.

Simplification

Adding a definition of scientific research could simplify the application of the GDPR.

However, the definition is so broad and at the same time unclear when it comes to research that is not aimed at technical innovation, that it does not deliver on simplification.

Data Subjects

Overall, the definition would limit or abolish data subjects' rights under Articles 5(1)(b) and (e), 9(2)(j), 14(5)(b), 17(3)(d) and 21(6) GDPR and (via Article 89(2) GDPR) also all rights under Articles 15, 16, 18 and 21 GDPR.

This means that basically all GDPR rights could be massively limited under such a broad "research" exemption.

Data subjects would have to engage in expensive procedures to overcome any claim of "research", especially in jurisdictions where Supervisory Authorities (SAs)do not engage with each complaint.

Controllers

Actual academic research in medicine, humanities or natural science may partly lose the current privileges in the GDPR, given that the definition would be limited to (technical) "*innovation*".

Controllers and processors could potentially abuse the definition to shield purely commercial processing activities from the GDPR. Especially processing of personal data for secondary purposes could be an area where the proposed definition could be broadly abused.

It is unclear how the definition would play out in practice, but it might allow for "*marketing research*" and application of knowledge in ways that are purely meant to help controllers to increase their revenue at the expense of fundamental data protection principles.

As with other unclear definitions, legal uncertainty would increase. and controllers and processors increasingly run the risk of high fines if their assessment is not confirmed by a supervisory authority or the courts.

Supervisory Authorities

Since there is a significant uncertainty and leeway in the definition of what could be considered scientific research, supervisory authorities would need further resources to investigate such claims.

The Supervisory Authorities would likely be tasked with evaluating the quality of the research suggested (Article 36(1)) or performed (Article 57(1)(f)) by the controller, as well as how well the research adheres to the principles suggested to apply to scientific research in recital 28 of the proposal.

Elements like private "ethics" rules for research would become (indirectly) applicable in GDPR cases.

Consequently, the suggested proposal would require supervisory authorities to evaluate and investigate matters far outside their core competence.

Real Life Examples

The new definition in Article 4(38) could be used by anyone claiming "innovation" and would thus allow for massive loopholes. For example:

- Section 42 of the Irish Data Protection Act just contains a blanket allowance to process any personal data for (undefined) "*scientific … research purposes*". This could now allow any company like Meta, Google or TikTok to just claim "*novel*" application of their knowledge or some other technology to widely bypass the GDPR.
- Already in 2014 Facebook engaged in "research" to detect when couples are likely to break up and was able to predict breakups two months before.
- Mastercard's business intelligence research could be considered "scientific research" when applied by controllers in for them novel ways.

Article 9(2)(k) & (5) - AI and Sensitive Data

Proposed Text

(k) processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, subject to the conditions referred to in paragraph 5.

5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such data. If removal of those data requires disproportionate effort, the controller shall in any event effectively protect without undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties.

Proposed Recitals

See also Recitals 30 and 31 on AI systems, that are printed below with Article 88c as they do not specifically refer to specially protected data under Article 9 GDPR.

(33) The development of certain AI systems and AI models may involve the collection of large amounts of data, including personal data and special categories thereof. Special categories of personal data may residually exist in the training, testing or validation data sets or be retained in the AI system or the AI model, although the special categories of personal data are not necessary for the purpose of the processing. In order not to disproportionately hinder the development and operation of AI and taking into account the capabilities of the controller to identify and remove special categories of personal data, derogating from the prohibition on processing special categories of personal data under Article 9(2) of Regulation (EU) 2016/679 should be allowed. The derogation should only apply where the controller has implemented appropriate technical and organisational measures in an effective manner to avoid the processing of those data, takes the appropriate measures during the entire lifecycle of an AI system or AI model and, once it identifies such data, effectively remove them. If removal would require disproportionate effort, notably where the removal of special categories of data memorised in the AI system or AI model would require re-engineering the AI system or AI model, the controller should effectively protect such data from being used to infer outputs, being disclosed or otherwise made available to third parties. This derogation should not apply where the processing of special categories of personal data is necessary for the purpose of the processing. In this case, the controller should rely on the derogations pursuant to Article 9(2)(a) – (j) of Regulation (EU) 2016/679.

Overview

The original arguments in the 1980ies to introduce principles like transparency, accuracy, data minimization, purpose limitation and alike were the foreseeable future, where untransparent algorithms would suck up the personal data of everyone and produce unforeseeable results that impact peoples' lives. Many of these descriptions are exactly what we today call "AI". It is therefore not surprising, that AI is limited by the very rules that were written to limit unintended consequences from such systems. Any changes to the GDPR must be seen with the original intention of the law in mind.

The Commission's proposal is meant to add a new legal basis to allow controllers to proceed to the processing of special categories of personal data (sensitive personal data). According to this legal basis the controllers can process sensitive personal data for the purposes of the development and operation of AI systems. This new sub-paragraph refers to the very broad definition of AI system according to Article 3, point (1) of Regulation (EU) 2024/1689 (AI Act).

In addition, the Commission proposes to add Article 9(5) GDPR, which sets out additional conditions for the processing of sensitive personal data. These conditions follow three steps:

- They include "*appropriate organisational and technical measures*" that should be put in place by the controller in order to avoid collecting and processing of special categories of personal data in general.
- Furthermore, if the controller "*identifies*" sensitive personal data in the already collected datasets, used for training, testing or validation of AI systems, they are obliged to remove the sensitive personal data.
- However, if the removal of the sensitive personal data requires disproportionate effort the controller should effectively protect the sensitive personal data from being used to produces outputs, be disclosed or otherwise used.

The key issue that arises is the lack of a documented proportionality assessment which should precede any limitation of a fundamental right according to Article 52(1) of the Charter. The Commission has only applied a "*reverse proportionality assessment*" which is conducted with a single sentence in the proposed Recital 33, all in favour of the controllers.

The AI allowance that the Commission proposes gives privilege to a certain type of technology and thereby leaves the "tech neutral" approach.

For the many other problems with the "AI" allowances in the draft, see below our analysis on Article 88c.

Charter

Any limitation of the rights under Article 8 of the Charter needs to be proportionate under Article 52 of the Charter. This new legal basis constitutes a limitation of the protection of personal data and would, therefore, would need to be accompanied by a proportionality assessment.

The draft text however seems to not only not provide for such an assessment, but actually seems to follow a "reverse proportionality test", that is only concerned with the controller:

- It does not seem that the Commission has ensured to have the necessary evidence to justify the need for such a limitation in the public interest (see e.g. the 50+ page assessment in the recitals on the EU-US data transfers to justify a Commission decision in light of Art 7, 8 and 47 of the Charter).
- Contrary to the legal duties of the legislator under Article 8 and 52 of the Charter, the new proposed Recital 33 seems to be only concerned with the law being disproportionate for the entity interfering with the right to data protection ("*In order not to disproportionately hinder the development and operation of AI* [...]").
- It is unheard of that the lack of a proportionality assessment is not just publicly documented, but that the legislator has apparently done a proportionality assessment for the wrong side – not the person protected by a fundamental right, but the person interfering with it.

While the text foresees "*appropriate organisational and technical measures*" there are currently no technical standards that would allow to objectively determine if a controller has implemented an "*appropriate*" measure.

The Commission proposes that processing activities that are conducted in the context of both the development and the operation of AI systems qualify for an exception from the high level of protection that the GDPR provides for sensitive personal data. While there is a debate that the training of personal data could be a legitimate interest, it would hardly be compatible with Article 8(1) and (2) of the Charter and would never "*survive*" a proportionality test under Article 52(1) of the Charter if the mere "*operation*" of a specific technology is by default legal, especially for sensitive data.

It also seems hard to explain under Article 8 and 20 of the Charter why the Commission has come to the conclusion that only one processing technology (AI) that traditionally involves higher risk for data subjects would meet the criteria of Article 8 of the Charter, while any other form of processing (such as a traditional database or a simple algorithm) would not be allowed under Article 9(2) GDPR.

Case Law

Please see our analysis on Article 88c for references to case law.

Legal Certainty

The proposed provisions provide a "privilege" for AI that goes beyond just training ("*development*"), but also the "*operation*" of an AI system.

This could mean, that processing is only legal if via an AI system, when a "traditional" database would not have a legal basis under Article 9(2). This would allow some kind of "AI wildcard", meaning controllers could start choosing to use AI technologies for processing activities because the exceptions under Article 9(2)(k) and (5) GDPR would now allow them to process sensitive personal data more easily.

The proposed provision lacks the necessary clarity and preciseness that is tied to the principle of legal certainty. For example:

- The controllers are asked to "*avoid*" the collection and processing of sensitive personal data, but this seems to have little practical meaning, especially in contexts that may naturally be inherently full of sensitive data (e.g. health data).
- Moreover, the controllers are obliged to remove residual sensitive data, unless it "*requires disproportionate effort*", which very unclear wording that has previously rendered provisions (e.g. in Article 14(5)(b) or 19 GDPR) totally meaningless in practice, because controllers claim such a "*disproportionate effort*" by default if large or unstructured data sets are involved.

The relevant Recital mentions that even just "re-engineering" of the AI system as an example of a disproportionate effort, but does not clarify what would be proportionate effort, especially in light of the fact that currently AI companies do not offer sufficient technical solutions for deletion or correction of wrong outputs.

According to the previously leaked version of the proposal, the controller would have to avoid the collection and processing of special categories "*to the greatest possible extent*". This phrase is now erased, resulting to greater legal uncertainty over the scope of this obligation to avoid the processing of sensitive personal data.

Legal Quality

The word "*operation*" is not defined. Usually the GDPR uses the word "*processing*" (as in Art 4(2) GDPR). It is unclear what "*operation*" would entail other than "*processing*", since this term is not included as a stand-alone term in the AI Act. This can itself create more legal uncertainty.

According to this proposal, the GDPR would refer to the extremely broad definition of the AI Act. While this may be useful to ensure consistent wording in EU law, in the context of the GDPR this has highly problematic effects:

- This broad definition was meant to have broad protections. When used for an exemption or legal basis, then it generates the opposite effect of a broad exemption.
- Because of the broad AI definition in the AI Act, many "*traditional*" processing activities would fall the exemption in the GDPR. Using this broad definition for an exemption would therefore lead to an extremely broad privilege in the GDPR that would go far beyond what is traditionally understood to be "AI".

As previously mentioned, paragraph 5 adds "*limitations*" to the use of sensitive data for AI training, which consist of a highly conditional ("*appropriate*") duty to "*avoid*" such collection or remove such information if it does not require "*disproportionate effort*".

Another wording that is not defined is the requirement for the controller to "*effectively protect*" the sensitive personal data from being used in outputs or otherwise being available to third parties, including disclosure.

Overall, the proposed provisions include vague and not sufficiently defined wording that would allow controllers to "stretch" the provision to a wide allowance to process sensitive personal data for any AI use.

Conflicts

The protection under Article 9(5) seems to be even weaker than the general data minimization principle in Article 5(1)(b) GDPR. It is unclear how these provisions relate to each other. It seems that the new Article 9(2)(k) would be largely consumed by Article 5(1)(b) GDPR.

Other than the provision for Article 6(1) data (see below Article 88c), this does not need a balancing test, but seems to be rather an absolute allowance with conditional protections. This would mean that sensitive data under Article 9 could have less protections that "normal" personal data. Overall, the protection system under Article 9 and 6(1) is not fully aligned, likely leading to more bureaucracy for controllers.

Elements in Recital 33 such as the fact that data may be processed that is "*not necessary*" indicate further structural intellectual and analytical errors given that "*necessary*" is an element of Article 6(1)(b) to (f) or Article 5(1)(c) GDPR or Article 52(1) of the Charter. This could easily allow a Challenge under Article 8 of the Charter, given that instead of any assessment the Recitals of the Legislator would show clear inconsistencies within the law and with the Charter.

Simplification

The proposed additions do not seem to address the technical complexity of artificial intelligence technologies and seems to add little to avoid any legal conflict between a controller, supervisory authority or data subject.

Data Subjects

Data subjects would have to be able to assess whether the controllers have put in the adequate level of effort according to the proposed Article 9(5) GDPR.

Currently most AI companies argue that the details of their data pipeline and selection of training data is "confidential", it would hence be very hard for data subjects to be able to proof that their rights under Article 9(5) GDPR were indeed protected.

The combination of a highly complex technical setup, likely confidentially claims, very vague language in the law and the huge power and information gap between controllers and data subjects in this area would make any enforcement of Article 9(5) GDPR highly unlikely. The practical value of such a provision is therefore questionable.

Controllers

The consequences for controllers and processors of an unclear legal situation usually depend on the individual situation of a company:

- For normal small or medium size controllers the unclear technical requirements, high costs to set up a three-level data cleaning approach, combined with massive legal uncertainty may make training (or fine tuning) of AI systems not overly attractive. Many small and medium-sized controllers could have to rely on larger players.
- Larger or "start-up" players will traditionally use the same legal uncertainty to entertain large legal teams to generate some form of "compliance circus" or will simply accept the risk of (later) enforcement action.

Overall, it is highly likely that most controllers would face a more complex and uncertain legal situation, while a small number of (aggressive or highly sophisticated) controllers may find ways to fully escape the application of the high threshold of protection that the GDPR provides for sensitive personal data.

Supervisory Authorities

Supervisory authorities would have to engage in deep technical investigations in order to determine if the controller has effectively avoided the collection and processing of sensitive personal data, whether they removed the data accordingly.

Unclear wording like if any additional measure would constitute a "*disproportionate effort*" could make enforcement action by supervisory authorities even more complex.

Overall, it seems questionable if supervisory authorities (with already strained budges and personal resources) will realistically be able to enforce this provision, lacking clearer rules.

Real Life Examples

Please see real life examples in our analysis of Article 88c.

Article 12(5) – Limitation - Right to Access

Current Text

(5) Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Proposed Text

(5) Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character **or also, for requests under Article 15 because the data subject abuses the rights conferred by this regulation for purposes other than the protection of their data,** the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating **that** the **request is** manifestly unfounded **or that there are reasonable grounds to believe that it is excessive** character of the request.

Proposed Recital

(35) Article 15 of Regulation (EU) 2016/679 provides data subjects with the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and certain additional information. The right of access should allow the data subject to be aware of, and to verify, the lawfulness of the processing and enable him or her to exercise his or her other rights under Regulation (EU) 2016/679. By contrast, it should be clarified in Article 12 of the Regulation that the right of access, which is from the outset favourable to data subjects, should not be abused in the sense that the data subjects abuse them for purposes other than the protection of their data. For example, such an abuse of the right of access would arise where the data subject intends to cause the controller to refuse an access request, in order to subsequently demand the payment of compensation, potentially under the threat of bringing a claim for damages. Other examples of abuse include situations where data subjects make excessive use of the right of access with the only intent of causing damage or harm to the controller or when an individual makes a request, but at the same time offers to withdraw it in return for some form of benefit from the controller. Moreover, in order to keep their burden to a reasonable extent, controllers should bear a lower burden of proof regarding the excessive character of a request than regarding the manifestly unfounded character of a request. The reason is that the manifestly unfounded character of a request depends on facts that lie principally within the controller's sphere of responsibility, whereas the excessive character of a request concerns the possibly abusive conduct of a data subject, which lies primarily outside the controller's sphere of influence, and therefore the controller may be able to prove such abuse only to a reasonable level. In any event, while requesting access under Article 15 of Regulation (EU) 2016/679 the data subject should be as specific as possible. Overly broad and undifferentiated requests should also be regarded as excessive.

Overview

This change seems to be inspired by a Paper of the German Government of 23 Oct 2025, based on a long-term debate in Germany about the use of Article 15 GDPR to gather evidence in civil court procedures. Given that more and more data is "sealed" from employees or customers in databases of controllers, people increasingly have to turn to access requests to overcome this information imbalance.

The amendment restrains the possibility for data subjects to use their right to access under Article 15 GDPR to get access to their own data, imposing that this right must be used for "*data protection purposes*". This would likely exclude journalistic, research, political, economic, legal or many other purposes to access one's own personal data.

This restriction is accompanied by a reduction of the controllers' burden of proof. They would be able to refuse to act upon the exercise of data subject rights when there are "*reasonable grounds*" to believe that the request is excessive. This could massively increase the already very high number of unjustified rejections of GDPR rights.

The amendment would provide for a concept comparable to purpose limitation but for data subjects' rights. This contradicts the fact that data protection should be seen as an "enabler" of other (fundamental) rights like the freedom of information and the academic freedom. It also violates existing CJEU case law, which likely means that it also violates Article 8(2) of the Charter that explicitly enshrines the right to access to personal data.

Charter

Article 8(2) of the Charter provides for the right to access (and to rectification) as a free-standing right. It is not an "annex right" and can therefore be used for any purpose, just like other Charter rights like the right to free speech or the right to property.

Article 52(1) of the Charter provides that limitations to the rights under the Charter must be provided by law if they are necessary and proportionate to the objectives of general interest or the need to protect the rights and freedoms of others.

Adding a condition to the exercise of the right provided by Article 8(2) of the Charter amounts to a restriction of the full application of the article. The Commission does not explain how such inference would be necessary or proportionate, especially given that the abuse of the access right (manifestly unfounded or excessive) is already covered in Article 12(5). This restriction will almost certainly not pass the proportionality test set out by the CJEU.

Given that the limitation to "*data protection purposes*" is also very vague (see below), there are also serious questions if the quality of law is sufficient for such a massive limitation.

Overall, the proposed change would lead to an (indirect) limitation of the right to an effective remedy in Article 47 of the Charter. Similar arguments can be made for economic, journalistic or research purposes, that are all recognized in the Charter.

There is no evidence that limiting the grounds for which an access request can be made so drastically is "*necessary*". Consequently, this is not lawful in accordance with Article 52 of the Charter.

Case Law

On the right to access as such, the CJEU consistently considered the right to access as a free-standing right, with no "purpose limitation":

- In C-307/22 *FT*, §§ 29 to 52, it was a question for a patient to have access to their dental file. The Court considered that the right to access could also be used when its purpose is different from those of Recital 63, 1st sentence, i.e. being aware of and verify the lawfulness of the processing.
- In C-579/21 *Pankki S*, § 88, the factual situation involved an access request in the context of a former employment relationship. The Court confirmed that the

context in which the data subject exercises their right to access cannot have any influence on the scope of that right.
- In C-526/24 *Brillen Rottler*, a person subscribed to a newsletter and then filed an access request with the controller. The controller refused to reply under Article 12(5) GDPR. In his opinion, the Advocate General recalled that the controller cannot require from the data subject to provide the reasons of the access request (§38). It then considered that the right of access is necessary to enable data subjects to exercise their right to compensation (§47).

The CJEU also consistently developed a strict balancing test when examining, under Article 52(1), the inference with a right under the Charter:

- In joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd*, the Court applied its balancing test and recalled that under the principle of proportionality, the acts of the EU institutions must be appropriate to attain the legitimate interest pursued by the legislation and not exceed the limits of what is appropriate and necessary (§46).
- The Court also developed a strict approach when applying its proportionality test in relation to inference to the right to data protection in C-473/12 *IPI* (§39).

Overall, the CJEU would have to come to the conclusion that under the GDPR there was no purpose limitation for access rights, but that under Article 8(2) of the Charter such a limitation may exist. This outcome is extremely unlikely. All available evidence shows that there is huge number of unlawful rejections and a very limited number of cases where evidence is further used for illicit purposes.

Legal Certainty

The amendment, read in light of the recital, reduces the controller's burden of proof when refusing to act on a request by a data subject or when charging a fee for taking action.

The controller only has to show that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive. This last concept is rather flexible and undermines the legal certainty both for the controllers, and for the data subjects:

- The controllers will perform subjective case-by-case assessments without clear guidelines.
- The data subjects have no clear view of the scope of their right given that it will largely be left to the discretion of the controller. As the assessment will be controller-specific, the right of the data subject will vary depending on the controller they will be dealing with.

The direct, though not explicitly pointed out by the Commission, opposition with the right under Article 8(2) of the Charter and with the well-established CJEU case law also adds to the confusion generated by the amendment.

Overall, on the data subject's right purpose limitation, the questionable legality of the amendment will have to be decided upon by the CJEU. On the burden of proof reduction, the amendment creates flexible concepts which will also need to be defined and clarified by Supervisory Authorities and the CJEU.

Legal Quality

The amendment creates a new ground to refuse acting upon an access request while there was no gap in the current text: There is already an exemption for abusive (manifestly unfounded or excessive) requests in Article 12(5) GDPR. And Article 15(3) GDPR protects rights and freedoms of others.

The potential factual consequences of the reduction of the burden of proof include:

- An actual shift of the burden of proof on the data subjects who will have to justify the data protection purposes of their requests;
- Systematic rejection of access requests.

Conflicts

The amendment clearly conflicts, as explained above, with the consistent CJEU case law and with the Charter.

The limitation of the right to access also conflicts with the very purpose of this right as an enabler of other rights, under the GDPR and under other legislation. The Commission itself recalled, in its Staff Working Document (p. 40), that one of the purposes of the right is to enable other rights.

Finally, the proposed limitation of access seems to conflict with the legislative objectives and related provisions established in other areas of EU law, where algorithms and data used by for example Very Large On-line Platforms (VLOPs) under the Digital Services Act and alike were increasingly made more transparent. Situations may arise where third parties (e.g. researchers) have more access to the personal data of Europeans than data subjects themselves.

Simplification

The flexible, case-by-case and subjective assessment creates confusion and uncertainty instead of simplification. Even though it may appear for controllers like an occasion to systematically reject access requests, the situation will likely end up being overthrown by the CJEU, who will apply the hierarchically superior Article 8 (2) of the Charter.

The Supervisory Authorities would also play a crucial role of interpretation, giving rise to the inevitable possibility of national variety in interpretation, all in all amounting to more confusion than with the current text.

For data subjects, the amendment, instead of simplifying their ability to request access (which, under the current text, is already jeopardized), creates complication and obstacles.

Data Subjects

Having access to information is a core element of the right to "informational self-determination". Using such data for other purposes than pure "data protection" purposes is not an "exploitation", nor an advantage given to the data subject to the detriment of the controller but the core right.

Informational self-determination is already impacted by increasing information imbalance: most evidence is not in "paper form" anymore (e.g. time sheets or communication), but digital (e.g. online systems, chatbots). It is therefore crucial that data subjects have an option to obtain copies for evidence purposes. Otherwise, the EU legislator would have to create hundreds of provisions to send copies of such digital evidence and agreements to consumers, to avoid an ever-increasing information imbalance.

The amendment condemns any request that has a motivation not directly related to the protection of personal data as "*abusive*". Indirectly (and in reality), this amendment would require data subjects to show their intention/motivation when making a request. A controller could just ask for the intent and say that non-disclosure of the purpose is a "*ground*" to "*believe*" that it may be used for a "*non data protection*" purpose.

The data subjects also suffer a limitation of their other rights. Even if the intent seems to be only narrowing the rights under Article 15 GDPR, it would lead to limitation of the other rights too as the right to access is widely used as a prerequisite to exercise other rights.

The recital also suggests that undifferentiated and general requests would be abusive. Controllers already regularly require data subjects to limit the scope of their requests to certain systems, but data subjects (naturally) do not have any knowledge about the processing systems of the controller and usually have little option other than to ask for "all data" to avoid controllers "hiding" problematic data by not disclosing where such data could be.

In conclusion, data subjects would see a clear diminution of their ability (already compromised under the current text) to exercise their right.

Controllers

Most companies hardly ever get an access request, some (e.g. data brokers) get a lot and therefore have automated the processing. There is a small group of "problematic" controllers that try to undermine access requests. The amendment will therefore benefit these bigger players with no real impact on SMEs.

As explained, the controllers will have to perform case-by-case assessments (which they will also need to document in prevision of litigation). That will take more resources. They will also inevitably face more complaints.

Supervisory Authorities

Problems encountered by data subjects when using Article 15 are already by far the most common reason for complaints. More reasons for rejections by controllers will likely lead to even more complaints.

The "*reasonable grounds to believe a request is excessive*" will also have to be defined by the Supervisory Authorities and likely by the CJEU.

In practice most access requests may "feel" excessive or at least annoying for a controller. This proposal is lowering the burden of proof immensely. Any (subjective) "*belief*" of a controller is probably reasonable, even if objectively not accurate.

While Supervisory Authorities are expected and used to make decisions based on facts, they will now have to assess the beliefs of the controllers and the purposes of the requests of the data subjects, two rather subjective concepts.

Real Life Examples

The right to access is already under very high pressure in daily practice, widely ignored and massively underenforced:

- Right now, gaining access can take upwards of 5 ½ years, even with large providers like YouTube and when enforcement is taking place. This reality is not remotely taken into account by the proposed amendment.
- In the experience of *noyb* at best 10% of access requests are yielding a (somewhat) full response within the legal deadline of one month. 90% of controllers fail to comply with Article 15.
- The online advertisement arm of Microsoft (Xandr) has given access to **0% (!)** of all access requests according to its own internal statistics that were leaked online.
- Many supervisory authorities do not properly enforce the right to access for each individual complaint, claiming that it would be impossible to enforce the right to access in each case already in the current form.

At the same time the right of access is widely used for many purposes and has a crucial role as a horizontal right to overcome information imbalance. Below is a short selection amongst the plenty of examples of real-life issues of the amendment:

- The right to access is widely used for evidence purposes, especially in employment context where i.e. in a dispute over unpaid hours, the data subject could request access to their digital time sheets. That would likely not qualify as a "*data protection purpose*".
- In the context of a loan given on the basis of a data subject's credit score, the data subject could request access to their data in order, subsequently, to delete or rectify false credit ranking data to get a cheaper loan at the bank, such rights may not be exercised purely for a "*data protection purpose*" but out of economic interest.
- In a lot of online-casino cases, data subjects get access to the history of their losses by means of an access request in order to claim them back because the online-casino was illegal. Such access requests would, according to the proposal, be excessive.
- This could lead to anyone being potentially in a conflict with a controller (e.g. employees, consumers, researchers or journalists) to be told that there are "*reasonable grounds*" that an access request is used for other purposes than for "*data protection purposes*". The exemption could therefore *de facto* become the default rule.

Furthermore, there are many other situations where access to personal data (as a horizontal

right to overcome information imbalance) enables other Fundamental Rights:

- Many forms of manipulation of the democratic process were proven by access to personal data on platforms.
- Regarding the freedom of information under Article 11 of the Charter. Making an access request to a big tech platform in order to write a journalistic paper about the business practices of said tech platform could be seen as having a purpose other than data protection and therefore rejected.
- The same is true in case an access request is made in course of academic research in accordance with Article 13 of the Charter.
- Access requests can also disclose structural inequality, discrimination and alike.
- In our practice there are many more cases where controllers "manifestly" do not comply with Article 15, than users abusing the right for other purposes.

Article 13(4) - Exception to Privacy Policy

Current Text

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Proposed Text

4. Paragraphs 1, 2 and 3 shall not apply where ~~and insofar as~~ **the personal data have been collected in the context of a clear and circumscribed relationship between data subjects and a controller exercising an activity that is not data-intensive and there are reasonable grounds to assume** that the data subject already has the information **referred to in points (a) and (c) of paragraph 1, unless the controller transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35.**

Proposed Recital

(36) Article 13 of Regulation (EU) 2016/679 requires the data controller to provide the data subject with certain information on the processing of his or her personal data as well as certain further information necessary to ensure fair and transparent processing, as defined in paragraphs 1, 2 and 3 of that provision. According to paragraph 4 of Article 13 of Regulation (EU) 2016/679, that obligation does not apply where and insofar as the data subject already has the information. To further reduce the burden of data controllers, without undermining the possibilities of the data subject to exercise his or her rights under Chapter III of the Regulation, this derogation should be extended to situations where the processing is not likely to result in a high risk, within the meaning of Article 35 of the Regulation, and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1 in the light of the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller. These should be the situations where the context of the relationship between the controller and the data subject is very clear and circumscribed and the controller's activity is not data-intensive, such as the relationship between a craftsman and their clients, where the scope of processing is limited to the minimum data necessary to perform the service. The controller's activity is not data-intensive where it collects a low amount of personal data and its processing operations are not complex, which is not the case, for example, in the field of employment. In such circumstances, that is to say when the processing is non data-intensive, non-complex and where the controller collects a low amount of personal data, it should be reasonable to expect, for instance, that the data subject has the information on the identity and contact details of the controller as well as on the purpose of the processing when that processing is carried out for the performance of a contract to which a data subject is a party, or when the data subject has given his or her consent to that processing, in accordance with the requirements laid down in Regulation (EU) 2016/679. The same should apply to associations and sport clubs where the processing of personal data is confined to the management of membership, communication with members and the organisation of activities. Nevertheless, this derogation from the obligations of Article 13 is without prejudice to the independent obligations of the controller under Article 15 of that Regulation, which applies in case the data subject requests access based on the latter provision. Where the derogation from the obligations of Article 13 does not apply, in order to balance the need for completeness and easy understanding by the data subject, controllers may adopt a layered approach when providing the information required, notably by allowing users to navigate to further information.

Overview

The Commission's proposal amends the exemption from the controller's information obligation under Article 13(4) GDPR. The proposal is meant to apply to SMEs (even though the wording of the proposal is not limited by size of the controller) and tries to describe a particular processing situation in which the controller should be exempted from its obligation to inform the data subject about the processing of their personal data. In order for this proposed exemption to apply the following conditions must be met:

- the personal data must be collected "*in the context of a clear and circumscribed relationship between data subjects and a controller*";
- the controller must exercise "*an activity that is not data-intensive*";
- there are "*reasonable grounds to assume*" that the data subject already has the information referred to in Article 13(1)(a) and (c) GDPR.

At the same time there are four counter-exemptions. Consequently, the exemption cannot be invoked by the controller, in case

- the controller transmits the data to other recipients or categories of recipients,
- the controller transfers the data to a third country,
- the controller carries out automated decision-making, including profiling, referred to in Article 22(1) GDPR, or
- the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35 GDPR.

Overall, the exemption seems to hardly apply to any SME, because almost any SME would usually use some processor (e.g. web hosting, email provider, hosting of CRM software, accounting software) that typically fall under the definition of a "recipient" in Article 4(9) GDPR. Furthermore, many of these recipients will operate outside of the EU/EEA or have in turn sub-processors that operate outside of the EU/EEA to provide the service, hence engaging in a transfer to a third country.

Charter

Processing must be done "*fairly*" under Article 8(2) of the Charter. While "*fairness*" and "*transparency*" are not the same, they are indeed closely linked.

For example, if a controller does not say which legal basis in Article 6(1) GDPR it operates under, it could hardly be seen as "*fair*" because the data subject would be unable to know if they have rights under Article 7 or 21 GDPR.

While limitations are possible, they must be proportionate under Article 52 of the Charter and "*provided for by law*", which requires a minimum of clarity and predictability, of such a limitation.

Case Law

There is no CJEU case law particularly dealing with the exemption of the information obligation under Article 13(4) GDPR.

Legal Certainty

This proposed amendment uses vague wording, enabling misuse and creating legal uncertainty.

The wording is extremely unclear and unpredictable: For example, it is unclear, what a "*clear and circumscribed relationship*" between the data subject and the controller is or what would constitute a "*not data-intensive*" „*activity*". There is not a single objective or hard condition in the provision (like affected data subjects).

For example: *noyb* processes around 25,000 email addresses for various newsletters. Is this a "*circumscribed relationship*" (given that this is

partly random people singing up to a newsletter) and not "*data intensive*" (given that this is the data of a small town) or is signing up to a newsletter such a simple and obvious situation that it would fall under the exemption? If *noyb* made the wrong assessment, it would be liable of up to €20 million in fines.

According to the Recitals, the added exception is supposed to cover, *inter alia*, the relationship between a craftsman and their clients. However, the wording of the provision could also be interpreted more broadly. It has absolutely no element that would refer to the size of a controller or the number of affected persons.

Similarly, the exemption is applicable in case "*there are reasonable grounds to assume that the data subject already has the information*". It is unclear when such reasonable grounds could be assumed.

Legal Quality

According to Recital 36 of the proposal, the amendment is supposed to extend the current exemption from the information obligation in Article 13(4) GDPR (i.e. cases where the data subject already has the information).

However, the text would (according to the proposal) replace the existing exemption. Therefore (and probably not intended by the Commission) in case the data subject already has the information listed in Article 13(1) and (2) GDPR, the controller cannot invoke the exemption in Article 13(4) GDPR unless the additional introduced conditions are met. It is unclear if the Commission wanted to add a new Article 13(5) GDPR here and simply made a numbering error?

Drafted as it is right now, the proposal would drastically reduce the circumstances in which a controller can invoke an exemption from its information obligation.

Conflicts

Some information listed in Article 13 GDPR (e.g. the legal basis for processing) are not covered by Article 15 GDPR because the legislator assumed that Article 15 does not require it – because people got that information already. The change is therefore at odds with the structure of the law.

Since the information is also not required to be known by the data subject in order for the proposed amendment to apply, the data subject would not be able to receive this information at all. Consequently, this would make the exercise of rights impossible (e.g. withdrawal of consent or an objection if the basis for processing is not disclosed).

This could be seen as a limitation of the rights under Article 8 of the Charter that is not proportionate. However, we assume that completely withholding information about the legal basis from the data subject was not the intention of the proposal (it even requires "*reasonable grounds to assume that the data subject already has the information*" – but not that it actually has the information) and assume that this is due to shortcomings in the legal quality of the draft.

The provision seems to be applicable in case the data subject consented to the processing (and the other requirements in the provision are fulfilled) – however, it is unclear how a consent can be informed, as required under the GDPR, when the information under Article 13 GDPR is not provided in full. This poses a potential conflict between this exemption and the conditions for consent under Article 6(1)(a) GDPR in connection with Article 7 and 4(11) GDPR.

Simplification

The current regulatory approach in Article 13(4) GDPR is very simple. The data subject has to be informed about the processing of their data unless (and to the extent) the data subject does not already have the information.

The proposal intends to amend this straight forward provision by adding an exemption with

a very unclear scope and wording, 3 conditions, and 4 counter-exemptions.

In practice, it will be very hard to tell for controllers whether the conditions for the exemption are met, resulting in enormous risk for penalties.

It is doubtful that this would provide any simplification compared to the current situation where the information is simply provided in a standard privacy policy that is handed to the data subject.

It should further be noted that all the information has to be known by the controller anyway, the exemption only deals with the provision of the information to the data subject.

Data Subjects

The initial information of the data subject about the processing of their personal data is a requirement for fair and transparent processing under the GDPR. *Inter alia*, it is a requirement for the data subject to assess the lawfulness of the processing of their personal data and for the exercise of their data subject rights.

While the proposal targets processing situations in which the data subjects can already make some assumptions regarding the scope and extent of the processing activity, the proposal would deprive data subjects of the possibility to make an informed assessment (or just to confirm their assumption) at the time of the data collection.

The data subject's option to make such an assessment would require a prior access request, effectively eliminating their options regarding whether they even want to (and to which extent) provide personal data to the controller.

Finally, the proposal effectively eliminates the data subject's option to receive some necessary information from the controller (i.e. legal basis of the processing) in case the exemption is invoked.

It would therefore be more logical to e.g. allow controllers to provide information upon request or in a less formal way. Fully refusing the right to information seems to be an extreme solution.

Controllers

In practice, the proposed exception will be hardly applicable: almost all SMEs will have an external service provider for most IT needs (email, website, POS software, calendar or billing), given that especially SMEs usually do not run their own servers or software. The current provision excludes a controller that forwards data to a "*recipient*" (see Article 4(9 GDPR), which includes all typical types of "*processors*". Hence, upwards of 99% of SMEs would be unable to use this provision.

The fact that in practice Article 13(4) GDPR would have basically no application in practice again raises questions as to the impact assessment and evidence for the proposed changes.

But even if the exemption would apply to a controller in practice, the proposal would likely shift the provision of information from the privacy policy to access requests. The only way for the data subject to receive the (other) information mentioned in Article 13 GDPR would be to make an access request to the controller under Article 15 GDPR. This might leave the controllers with even more work.

Supervisory Authorities

Supervisory Authorities often consider the controller's privacy policy during their investigations. The implementation of the proposal would result in less privacy policies being provided to data subjects, meaning that also the Supervisory Authority will have less opportunity to consult the controller's privacy policy.

The lack of any upfront paper proof of purposes, legal basis and alike allows controllers to (later) shift their story in any investigation.

While investigating a controller's failure to provide information to a data subjects under Article 13 GDPR is rather simple for the Supervisory Authority under the current regime, the proposal will make this much harder, providing for complex questions the Supervisory Authority has to consider in its investigations.

E.g., was the data collected in the context of a clear and circumscribed relationship between data subjects and a controller? Is the processing an activity that is data-intensive, or does it pose a high risk for the data subject?

Real Life Examples

While the exemption is clearly intended for situations such as a craftsman providing a service to its customer, it is hard to see that many craftsmen will engage in a vague legal analysis with seven (!) elements to proof to avoid handing out a privacy policy. In simple terms: filling out a template for a privacy policy may be simpler than applying Article 13(4) GDPR.

It is foreseeable that this exemption could be used extensively by actors with an interest in keeping their processing opaque – and therefore have an interest in not providing information to the data subjects.

At the time of the collection of personal data, it will regularly be impossible for the data subject to tell, whether the controller failed to provide the initial information about the processing activity in violation of Article 13 (1) and (2) GDPR or whether the exemption is applicable.

Article 13(5) - Limitation of Right to Access

Proposed Text

(5) When the processing takes place for scientific research purposes and the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing, the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

Proposed Recitals

(37) Where the processing takes place for the purpose of scientific research and the provision of information to the data subject proves to be impossible or would involve a disproportionate effort it should not be necessary to provide the information provided for under Article 13 of this Regulation. The controller should make reasonable efforts to acquire contact details if they are readily available and acquisition would not require a disproportionate effort. The provision of the information would involve a disproportionate effort in particular where the controller at the time of collection of the personal data did not know or anticipate that it would process personal data for scientific research purposes at a later stage, in which case it may not have easily available contact details of the data subjects. In such situations the controller should inform data subjects indirectly, such as by making the information publicly available. The provision of such information should ensure that as many data subjects concerned as possible are reached. Relevant means to make the information publicly available should be determined depending on the context of the research project and the data subjects involved.

Overview

The Commissions suggestion to limit the right to information about data processing when the processing is done for scientific purposes is an addition to the GDPR. Recital 37 suggest ("*where the controller … did not … anticipate that it would process personal data for scientific research purposes*") that this aims at situations where personal data was obtained from the data subject, but is now used for a different, secondary "*scientific research*" purpose, so a situation where under Article 13(3) GDPR an active information about the change of purpose is required. In the current system, data subjects can then in turn challenge unlawful further use, or exercise their right to object under Article 21(6) GDPR. Without such information, the rights of data subjects can *de facto* not be exercised.

In light of the extremely broad new definition of "*scientific research*" under the proposed Article 4(38) and the fact that the purpose limitation principle in Article 5(1)(b) does not apply to processing for scientific research purposes, this change would make originally unintended secondary processing substantially less transparent.

The derogations from the right to information follow the same pattern as Article 14(5)(b) GDPR for situations where there is no direct contact between controllers and data subjects. Namely that if:

- providing information is impossible,
- requires disproportionate effort or
- if the aims of the processing are impaired or made impossible,

then the obligation to provide information directly under Article 13 GDPR ceases to exist, but instead the controller must take "*appropriate*" measures, including publishing the information.

The suggested exception from rights seem to specifically designed to enable controllers to process data for scientific research purposes in situations where for example the controller no longer has a relationship with the data subject.

Charter

During the negotiations on the GDPR, one argument why Article 6(4) and various limitations of the principle of purpose limitation in Article 5(1)(b) GDPR would be compliant with the fundamental rights under Article 8(2) of the Charter (which includes "*purpose limitation*"), was that under Article 13(3) GDPR, data subjects must be at least actively informed about any such change of purposes.

Given that many other provisions of the GDPR link to the originally set "*purpose*", it serves as a major "backbone" of the intellectual and logical construct of the GDPR.

Removing these active information obligations, takes away a key element that could be used to explain why such a limitation of Article 8(2) is still "*proportionate*" under Article 52(1) of the Charter. Such a change must therefore be considered under the bigger picture of an increasingly intransparent and unregulated violation of the purpose limitation principle in Article 8(2) of the Charter.

See comment on Article 13(4) above on the interplay of transparency, "*fairness*" and Article 8(2) of the Charter.

Case Law

We did not find relevant case law particularly dealing with the exception to the information obligations under the similar provision in Article 14(5) GDPR.

Legal Certainty

This proposed amendment uses similar wording as the existing exception in Article 14(5)(b) GDPR for situations where there is no direct contact with a data subject. This could in principle help with legal certainty.

From a data subject's perspective, the lack of any active information about the change of processing purposes is a major problem for legal certainty. It undermines the core concept of the GDPR under "*purpose limitation*" that data subjects provide data for a specific purpose – and generally can trust personal data is not used for unforeseen purposes. This trust is enshrined in Article 8(2) of the Charter.

Passive information (e.g. a privacy policy on a website of a research institution that the data subject has never had any contact with) does not ensure that the data subject has any realistic path towards challenging such secondary use or to even just exercise rights, like under Article 21(6) GDPR.

In combination with the proposed Article 4(38), data subjects could lose any trust that personal data once provided (e.g. on a Social Network many years ago) is not used for some commercial "*innovation*" that was neither foreseeable nor accepted by the data subject.

Legal Quality

See above on Article 4(38) for the legal quality issued in the new definition of "*scientific research*".

Conflicts

The proposed law is a direct conflict with the logic under Article 13(3) GDPR to provide information if there is a change of purpose (such as a secondary use for "*scientific research*") to overcome the interference with Article 8(2) of the Charter.

Furthermore, it conflicts with the logic under Article 21(6) GDPR, which provides for an option to object to further processing for scientific research purposes – structurally such an objection required previous information of the data subject.

Beyond the GDPR and law, not informing data subjects about the use of their data also conflicts with basic scientific standards. See for example the European code of conduct for research ethics: "*Researchers inform research participants about how their data will be used, reused, accessed, stored, and deleted, in compliance with GDPR.*"

Simplification

For data subjects there would be a need to actively "hunt" for information regarding secondary use of personal data by controllers that they may not have interacted with in decades. This is anything but a simplification from an individual's perspective.

The suggested wording in Article 13(5) on the other hand would limit the information obligations of controllers regarding secondary processing for (board) research purposes.

In essence it would allow controllers who had a direct relationship with a data subject to engage in secondary use of data for "*scientific research*" even after the relationship between data subject and controller has ceased and without informing them about such further use.

Data Subjects

With the broad new definition of scientific research as proposed by the Commission in Article 4(38), the exception from the right to information is likely to lead to a substantial loss of data subjects' control over their personal data, as they cannot trust that controllers would only use their personal data for the previously specified purpose – or at least inform them about any intended changes.

Controllers

For controllers the combination of Article 4(38) and the increasing options to go "dark" about secondary use of personal data in "*innovative*" or "*novel*" ways opens a major loophole.

Supervisory Authorities

For supervisory authorities, enforcement of (unlawful) secondary use may get increasingly hard, if controllers do not have to inform data subjects about such a secondary use. The lack of information in privacy policies may also provide increasingly less paper evidence – requiring ever more complex factual investigations.

Real Life Examples

The exception (in combination with the new definition in Article 4(38) GDPR) seems tailored to legitimize controllers processing personal data they have collected for secondary AI training, such as the secondary use by Facebook, LinkedIn or "X" (formerly Twitter).

Article 22(1) & (2) – ADM

Current Text

(1) The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

(2) Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

Proposed Text

1. A decision which produces legal effects for a data subject or similarly significantly affects him or her may be based solely on automated processing, including profiling, only where that decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller **regardless of whether the decision could be taken otherwise than by solely automated means;**

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

Proposed Recitals

(38) Article 22 of Regulation (EU) 2016/679 provides for rules governing the processing of personal data when the data controller makes decisions which have legal effects or similarly significant effects on the data subject, based solely on automated processing. In order to provide greater legal certainty, it should be clarified that decisions based solely on automated processing are allowed when specific conditions are met, as set out in Regulation (EU) 2016/679. It should also be clarified that when assessing whether a decision is necessary for entering into, or performance of, a contract between the data subject and a data controller, as set out in Article 22(2)(a) of Regulation (EU) 2016/679, it should not be required that the decision could be taken only by solely automated processing. This means that the fact that the decision could also be taken by a human does not prevent the controller from taking the decision by solely automated processing When several equally effective automated processing solutions exist, the controller should use the less intrusive one.

Overview

The Commission's proposal merges paragraphs 1 and 2 of Article 22 GDPR into one paragraph. On the surface, paragraph 1 seems to be materially unchanged even if it is formulated differently - not as a right but as cases in which automated decision-making (ADM) is permitted.

The (only) material change is connected to the permission to use ADM in case of "*necessity*" for entering into, or performance of, a contract. This should be the case regardless of whether the decision could be taken otherwise than by solely automated means.

While generally the term "*necessary*" is not understood to mean that digital processing must always be replaced by "*pen and paper*" if this is possible, it means that there must be no less intrusive methods to achieve the purpose of the processing. Accordingly, the current version of Article 22(2)(a) GDPR stipulates that "*the controller must be able to show that this type of processing* [ADM] *is necessary, taking into account whether a less privacy-intrusive method could be adopted*." (see Article 29 guidelines p 23).

The proposed amendment seems to abandon this principle. In the future, it should not matter for the assessment of necessity whether the decision could also be taken by not solely automated means.

Charter

Generally, Article 22 GDPR (i.e. the right not to be subject to automated individual decision-making) is not laid down in the Charter.

However, the principles of necessity and proportionality under Article 52(1) of the Charter are engaged whenever a controller interferes with the right to data protection. Therefore, the term "*necessity*" must be interpreted in line with the meaning given to it in Article 52(1) of the Charter.

Furthermore, already Article 9(1)(a) of the Council of Europe's Convention 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) provided for the right of data subjects "*not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration*".

Case Law

The CJEU provided clarifications regarding the scope of Article 22 GDPR in CJEU C-634/21 *SCHUFA*. Part of the legal certainty that was created could be lost due to the amendments to the text of the provision – at least unless the CJEU clarifies that the amendment to the current version of Article 22(2)(a) of the GDPR did not materially change the provision.

Legal Certainty

Regarding the right not to be subject to certain processing activities involving ADM (current Article 22(1) GDPR), the CJEU's case law already provided for valuable clarifications.

Insofar as the Commission's draft is supposed to provide "*greater legal certainty*" (Recital 38), it fails to do so:

- Article 22(2) GDPR already allows for ADM in certain cases; therefore, the change in wording (seemingly) provides no material change. However, for practitioners it may create legal uncertainties (e.g. whether the CJEU case law is still applicable for the amended provision). Similarly, changing the wording in a way that no longer provides for a data subject right, while maintaining the provision in Chapter III (Rights of the data subject) provides further uncertainty regarding the nature of Article 22 GDPR.
- Further, the amendment to the current version of Article 22(2)(a) GDPR (i.e. excluding the question whether a decision could also be taken without ADM from the assessment of necessity) raises the question whether the requirement of necessity in that provision still adds anything (and if so, what) to the already existing requirement of Article 6(1)(b) GDPR. Since any decision taken under Article 22 also needs a legal basis in Article 6(1) GDPR (see CJEU C-634/21 *SCHUFA* §67 et seqq) which similarly provides for the requirement of necessity.

Legal Quality

Article 22 GDPR was generally considered to be of limited legal quality, and was often seen as difficult to understand. Simplifications of the text are therefore generally welcome.

Article 22(3) and (4) GDPR refer to other paragraphs of Article 22 GDPR. The Commission's proposal fails to make the necessary amendments to these references.

Also, Article 22 GDPR provides for the prohibition of ADM with certain exceptions (this applied to both the current and the proposed version). Phrasing this as a permission in certain cases ("*may be based solely on automated processing […] only where …*") is technically inferior (less understandable) than providing for a prohibition of ADM first and then exemptions to this prohibition.

Conflicts

While the amendment of Article 22 GDPR no longer provides for a data subject right not to be subject to ADM,the provision is still embedded in Chapter II (Rights of the data subject) and Article 12(2) GDPR still refers to Article 22 GDPR as a right of the data subject. The proposed amendment therefore potentially tears apart this puzzle pieces, creating a potential conflict between these provisions.

The amendment to the requirement of necessity in the current version of Article 22(2)(a) GDPR conflicts with the general principle that the controller should use the least intrusive means for processing, since the amendments give controllers full discretion as to the use ADM, even if a less intrusive alternative would be just as effective.

Simplification

The amendment to the wording of Article 22(1) GDPR (i.e. the rephrasing of the provision from a data subject's right to a permission in certain cases) seems to be a purely linguistic amendment without materially changing the scope of the provision – in contrast to the proposed amendment regarding the necessity in the current Article 22(2)(a) GDPR.

On the other hand, the amendment to the requirement of necessity for entering into, or performance of, a contract between a data subject and a data controller does indeed provide some simplification for controllers, given that the assessment of whether the decision could also be taken with other (less invasive) means than solely automated decision making may be disregarded by controller – or at not investigated to the same extent as currently. This is however "simplification" at the expense of individuals subjected to such decisions.

Data Subjects

ADM (e.g. account suspensions, declines to enter into a contract) is increasingly frequent and is considered enormously frustrating by data subjects.

The proposed amendment may accelerate this development: According to this proposal, controllers appear to have increased discretion as to whether to use ADM for the performance of, or entering into, a contract. This is quite a political paradigm shift, whichmay lead to greater usage of ADM, subjecting data subjects to automated decisions without (prior) human involvement.

Even with the current version of the provision, the lack of human involvement in the decision making is already problematic, since many controllers using ADM have an overall strategy of ideally "not interact" with consumers. This means that protections under Article 22(3) GDPR are regularly unavailable or meaningless in practice (automated email response, signed by a generic name).

Therefore, being more often subject to ADM will certainly have a significant impact on individuals' rights and freedoms, considering how often algorithms still show an immense degree of bias and are often unexplainable and, as a result, can produce unfair, unreliable and incomprehensible results.

Controllers

Besides the increased legal uncertainty created by the proposed amendment (see above), controllers and processors would be able to perform more processing activities in a fully automated manner without any human involvement.

Supervisory Authorities

The proposed amendment would not lead to any significant foreseeable changes for Supervisory Authorities.

Real Life Examples

Fully automated rejections by business when consumers want to enter into a contract would become potentially more common. Similarly, fully automated selection processes for jobs, schools, universities etc. would become even more prevalent.

Article 33 - Data Breach Notifications

Current Text	Proposed Text
1. In 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 competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.	In the case of a personal data breach **that is likely to result in a high risk to the rights and freedoms of natural persons,** the controller shall without undue delay and, where feasible, not later than ~~72~~ **96** hours after having become aware of it, notify the personal data breach **via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555** to the supervisory authority competent in accordance with Article 55 **and Article 56.** ~~unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.~~ Where the notification to the supervisory authority is not made within ~~72~~ **96** hours, it shall be accompanied by reasons for the delay.
Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.	1a. Until the establishment of the single-entry point pursuant to Article 23a of Directive (EU) 2022/2555, controllers shall continue to notify personal data breaches directly to the competent supervisory authority in accordance with Article 55 and Article 56.
	(...)
	6. The Board shall prepare and transmit to the Commission a proposal for a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as for a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person. The proposal shall be submitted to the Commission within [OP date = nine months of the entry into application of this Regulation]. The Commission after due consideration reviews it, as necessary, and is empowered to adopt it by way of an implementing act in accordance with the examination procedure set out in Article 93(2).
	7. The template and the list referred to in paragraph 6 shall be reviewed at least every three years and updated where necessary. The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6.

Proposed Recitals

(39) In order to reduce the burden on controllers while ensuring that supervisory authorities have access to the relevant information and can act on violations of the Regulation, the threshold for notification of a personal data breach to the supervisory authority under Article 33 of Regulation (EU) 2016/679 should be aligned with that of communication of a personal data breach to the data subject under Article 34 of that Regulation. In the case of a data breach that is not likely to result in a high risk to the rights and freedoms of natural persons, the controller should not be required to notify the competent supervisory authority. The higher threshold for notifying a data breach to the supervisory authority does not affect the obligation of the controller to document the breach in accordance with paragraph 5 of Article 33 of Regulation (EU) 2016/679, or its obligation to be able to demonstrate its compliance with that Regulation, in accordance with Article 5(2) of that Regulation. In order to facilitate compliance by controllers and a harmonised approach in the Union, the Board should prepare a common template for notifying data breaches to the competent supervisory authority and a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person. The Commission should take due account of the proposal prepared by the Board and review them, as necessary, prior to adoption. In order to take account of new information security threats, the common template and the list should be reviewed at least every three years and updated where necessary. The lack of a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person should not affect the obligations of controllers to notify those breaches.

Overview

The Commission's draft establishes that the so-called "single-entry point", after its establishment, should be notified about data breaches. The EDPB should prepare a proposal for a common template for data breach notifications as well as a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person (i.e. triggering the notification obligations).

The amendment to Article 33(1) GDPR would raise the threshold for the obligation to notify the Supervisory Authority about a data breach, going from the current text of Article 33 "*unless [it's] unlikely to result in a risk …*" to the prosed text "*[it's] likely to result in a high risk*". The change is therefore twofold:

- the threshold is moved from "*a risk*" to "*high risk*", and
- the exemption ("*unlikely*") is turned into a condition for the duty to kick in ("*likely*").

While the high number of Data Breach Notifications (e.g. wrongly sent emails) has led to supervisory authorities generally often just ignoring them, the change seems to be quite significant. So far Article 34 GDPR requires a direct information of data subjects about a data breach in case of a "*high risk*" – which hardly ever happens. The proposal would shift from the current obligation to notify the supervisory authority about almost every incident to a situation in which almost no incident will be reported to the supervisory authority.

The proposal also prolongs the deadline for the notification from 72 to 92 hours.

Charter

The obligation to inform the Supervisory Authority (or some other contact point) under Article 33 GDPR cannot be found directly in the Charter.

However, Article 7(2) of Convention 108 (Convention for the protection of individuals with regard to the processing of personal data) provides for the controller's obligation to notify "*at least*" and "*without undue delay*" the competent supervisory authority of a data breach which may seriously interfere with the rights and fundamental freedoms of data subjects.

Case Law

There is no CJEU case law particularly relevant for the proposed amendment.

Legal Certainty

Furthermore, the threshold of a "*hight risk*" is still unclear, which becomes even more urgent to solve, given that supervisory authorities would now not be able to do a second assessment under Article 34(4) GDPR.

Legal Quality

Regarding the preparation of a list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person, the proposal fails to clarify that such list only has an indicative effect or that if the conditions set out are met, a notification has to be made but not meeting the conditions does not mean that no notification has to be made.

Other than that, we did not investigate the legal quality of this particular provision further.

Conflicts

The level for the obligation to notify the Supervisory Authority would be effectively raised to the level of the notification of data subjects in Article 34 GDPR: the wording of Article 33 GDPR would then be 1:1 the same as Article 34 GDPR.

It is well-known that the number of notifications under Article 33 GDPR was a multitude compared to notifications under Article 34 GDPR. If the current number of Article 34 notifications is taken as a realistic benchmark for future data breach notifications to Supervisory Authorities, we would see only the most extreme breaches reported.

The 1:1 same threshold would undermine the current logic of Article 33 and 34, where in a first step the Supervisory Authority is in many more cases informed and only in a second step a controller also has to inform data subjects in a case where a "*high risk*" exists.

This would typical also make Article 34(4) GDPR void since the cases where only the Supervisory Authority has to be notified but not the data subjects would be limited to the cases Article 34(3) GDPR.

The notion to limit the reporting on trending issues around cybersecurity risks seems to conflict with the efforts of the EU in other laws to increase the Member State's awareness of such risks and increased data and intelligence sharing.

Simplification

While the extension of the notification deadline reduces the urgency in case of a data breach, the controller is still required to document each data breach (see Article 33(5) GDPR), its respective evaluation, and remedial actions taken.

Even if no notification of the supervisory authority is necessary, it is not clear whether this amendment would indeed provide any simplification beyond the receiving authorities.

Data Subjects

On a regular basis, controllers mischaracterise a data breach as not being "high risk" and only notify the Supervisory Authority. The Authority can then in turn order the controller to also inform all data subjects because it finds an initially incorrect assessment of the risks by the controller. The Commission's proposal will effectively eliminate the data subject's notification in such cases, because the notification to Supervisory Authority under Article 33 and the notification to data subjects under Article 34 GDPR now would have the same threshold.

Also, data subjects might be affected by a decrease in cybersecurity since the Supervisory

Authority could no longer provide guidance to controllers in case of data breaches with low to medium risk.

Controllers

Controllers would lose their "face saving way" to reach a supervisory authority in case of an incident. Given that the threshold for reporting ("*high risk*") would be the same under Article 33 and 34 GDPR, any acceptance that a report to the supervisory authority is warranted would typically also trigger Article 34.

Because controllers are typically reluctant to notify data subjects due to the immense potential consequences of such a notification (damages claims, reputational harm), this could lead to a psychological effect, that almost no data breaches will be reported anymore, because any compliance with Article 33 would be "penalised" with also the triggering of Article 34.

Such a dynamic may in turn increase the likelihood of further damages and leave controllers alone in a situation where many controllers may need support by authorities.

However, controllers (as well as their processors) will welcome the prolongation of the deadline to submit a data breach notification to 96 hours as well as the provision of templates for data breaches.

Supervisory Authorities

Supervisory Authorities would receive significantly less notifications, especially on tiny violations that were so far overwhelming SAs.

However, they would also lose crucial information on broader cybersecurity risks – which could be used to limit further breaches and ensure a full picture of broader attacks or problems.

It also takes away the Supervisory Authorities' ability to assess whether a controller correctly assessed the risk connected to a data breach (unless the result already was a high risk).

Real Life Examples

The change will likely have a big effect in cases where controllers (falsely) claim that there is no high risk, as supervisory authorities would lose their options to order a breach notification to affected data subjects. This is a rather regular situation. For example:

- In Decision 10070521 by the Italian SA, a bank was affected by a data breach affecting thousands of its customers. The bank notified the supervisory authority as required under Article 33 GDPR, but considered the data breach not to result in a "*high risk*" to the rights a freedoms of data subjects. However, the Supervisory Authority clarified that the data breach indeed posed a "*high risk*" for the affected clients and ordered the controller to directly notify the data subjects under Article 34 GDPR.

Article 35 – DPIAs

Current Text

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

Proposed Text

4. The Board shall prepare and transmit to the Commission a proposal for a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.

5. The Board shall prepare and transmit to the Commission a proposal for a list of the kind of processing operations for which no data protection impact assessment is required.

6. The Board shall prepare and transmit to the Commission a proposal for a common template and a common methodology for conducting data protection impact assessments.

6a. The proposals for the lists referred to in paragraphs 4 and 5 and for the template and methodology referred to in paragraph 6 shall be submitted to the Commission within [] months of the entry into application of this Regulation. The Commission after due consideration reviews them, as necessary, and is empowered to adopt them by way of an implementing act in accordance with the examination procedure set out in Article 93(2).

6b. The lists and the template and methodology referred to in paragraph 6a- shall be reviewed at least every three years and updated where necessary. The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6a.

6c. Lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data protection impact assessment is required established and made public by supervisory authorities remain valid until the Commission adopts the implementing act referred to in paragraph 6a.

Proposed Recitals

(40) Article 35 of that Regulation (EU) 2016/679 requires controllers to conduct a data protection impact assessment where the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons. The supervisory authorities established pursuant to that Regulation are required to establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. In addition, the Regulation provides that supervisory authorities may establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. In order to effectively contribute to the aim of convergence of the economies and to effectively ensure free flow of personal data between Member States, increase legal certainty, facilitate compliance by controllers and ensure a harmonised interpretation of the notion of a high risk to the rights and freedoms of data subjects, a single list of processing operations should be provided at EU level, to replace the existing national lists. In addition, the publication of a list of the type of processing operations for which no data protection impact assessment is required, which is currently optional, should be made mandatory. The lists of processing operations should be prepared by the Board and adopted by the Commission as an implementing act. In order to facilitate compliance by controllers, the Board should also prepare a common template and a common methodology for conducting data protection impact assessments, to be adopted by the Commission as an implementing act. The Commission should take due account of the proposals prepared by the Board and review them, as necessary, prior to adoption. In order to take account of technological developments, the lists and the common template and methodology should be reviewed at least every three years and updated where necessary.

Overview

The Commission's proposal basically moves the obligation to establish black/white lists of the kind of processing operations that require (or that do not require) a data protection impact assessment (DPIA) from the supervisory authorities to the EDPB, which then submits the lists to the Commission. Further, the proposal allows the Commission to adopt such lists received by the EDPB.

We welcome that the proposed amendment would replace national rules and white- and blacklists with consistent Union-wide rules.

The approach of clear black/white lists aims at a system that is clear and easy to implement for controllers to avoid complex multi-factor "risk assessments".

Charter

Taking into account that the proposal does not affect the obligation to perform a DPIA itself, the Charter does not conflict with the Commission's proposal.

Case Law

There is no CJEU case law particularly relevant for the proposed amendment.

Legal Certainty

The proposal allows for white/blacklists if a DPIA is necessary.

This should replace national rules that were inconsistent or non-existent. Such a change has therefore the potential to increase legal certainty and consistency.

Legal Quality

Due to the scope of the proposed amendment, there seems to be no apparent problem as to the legal quality.

Conflicts

We understand that the Commission's amendments also take into account to required adjustments in the tasks of the Supervisory Authorities and the EDPB.

These matters were not examined in detail.

Simplification

Providing increased legal certainty would similarly provide for simplification for controllers – in particular in case a controller operates in different Member States and had to consider different White- and Blacklists from national Supervisory Authorities.

One union-wide version would simplify compliance for such a controller.

Data Subjects

Due to the limited scope of the proposed amendment, we consider that the effects on data subjects will be negligible.

Controllers

As mentioned above, the increase in legal certainty could be advantageous for controllers and limit the need to do complex "risk assessments" under Article 35(3) GDPR.

Supervisory Authorities

While Supervisory Authorities are relieved of the task to establish white / black lists themselves, they also benefit from the increased legal certainty provided by such lists established by the EDPB and adopted by the Commission.

Real Life Examples

Due to the limited scope of the Commission's proposal, the amendment is not suitable for any real-life examples.

Article 41a - Definition of "Personal Data"

Proposed Text

(1) The Commission may adopt implementing acts to specify means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities.

(2) For the purpose of paragraph 1 the Commission shall:
(a) assess the state of the art of available techniques;
(b) develop criteria and or categories for controllers and recipients to assess the risk of re-identification in relation to typical recipients of data.

(3) The implementation of the means and criteria outlined in an implementing act may be used as an element to demonstrate that data cannot lead to reidentification of the data subjects.

(4) The Commission shall closely involve the EDPB in the preparations of the implementing acts. The EPDB shall issue an opinion on the draft implementing acts within a deadline of 8 weeks as of the receipt of the draft from the Commission.

(5) The Implementing Acts shall be adopted in accordance with the examination procedure referred to in Article 93(3).

Proposed Recital

(27) This Regulation proposes a series of targeted amendments to Regulation (EU) 2016/679 for clarification and simplification, whilst preserving the same level of data protection. Article 4 of Regulation (EU) 2016/679 provides that personal data is any information relating to an identified or identifiable natural person. In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. Taking into account the case-law of the Court of Justice of the European Union concerning the definition of personal data, it is necessary to provide further clarity on when a natural person should be considered to be identifiable. The existence of additional information enabling the data subject to be identified does not, in itself, mean that pseudonymised data must be regarded as constituting, in all cases and for every person or entity, personal data for the purposes of the application of Regulation (EU) 2016/679. In particular, it should be clarified that information is not to be considered personal data for a given entity where that entity does not have means reasonably likely to be used to identify the natural person to whom the information relates. A potential subsequent transmission of that information to third parties who have means reasonably allowing them to identify the natural person to whom the information relates, such as cross-checking with other data at their disposal, renders that information personal data only for those third parties who have such means at their disposal. An entity for which the information is not personal data, in principle, does not fall within the scope of application of Regulation (EU) 2016/679. In this respect the Court of Justice of the European Union has held that a means of identifying the data subject is not reasonably likely to be used where the risk of identification appears in reality to be insignificant, in that the identification of that data subject is prohibited by law or impossible in practice, for example because it would involve a disproportionate effort in terms of time, cost and labour. An example of a prohibition against reidentification can be found in the obligations of health data users in Article 61(3) of Regulation (EU) 2025/327 of the European Parliament and of the Council35. The Commission, together with the European Data Protection Board, should support controllers in the application of this updated definition by stipulating technical criteria in an implementing act.

Overview

According to this newly proposed Article 41a, read in conjunction with the proposed Article 4(1) (see above), the Commission seeks to unilaterally define what constitutes "*unidentifiable*" pseudonymised data. We would assume that the Commission would be under intense political pressure to gradually allow more and more (questionable) techniques under such an instrument.

The proposed examination procedure would require the involvement of a committee composed of representatives of EU Member States, but would not involve the European Parliament. In practice, these committees have so far e.g. passed EU-US data transfer agreements that the European Parliament was highly critical of and the CJEU has later overturned.

Until now, all processing of "*identifiable*" individuals is still governed by the GDPR, including pseudonymised data. With easier classification of pseudonymised data, and the subsequent data not counting as "personal data" anymore (as seen in the proposed change of Article 4(1) GDPR), it would significantly narrow the scope of protection that the GDPR currently offers.

If successful, this action would change a core element of the GDPR and also shift key interpretive powers to the European Commission. As can be seen from the Implementing Decisions on Data Transfers, the Commission is a political actor where decisions are naturally based on broader political views.

The CJEU would however be able to overturn such decisions when the Commission has gone beyond the realm of the GDPR and the Charter. It is not unlikely that the core definition of the GDPR ("*personal data*") would get entangled in decades of litigation and legal uncertainty if such key definitions are interpreted by the Commission.

Furthermore, the option for the Commission to *de facto* interpret the key definition of the GDPR may also get into tension with Article 8(3) of the Charter, which foresees that the right to data protection is primarily enforced by independent supervisory authorities – and, under Article 78 and 79 GDPR, by independent courts.

Charter

The idea that the Commission can decide if certain technical implementations fall under the definition of "*personal data*" or not equates to the application of the law – at a core definition and with wide ranging implications.

However, compliance with the GDPR must be "*subject to the control by an independent authority*" under Article 8(3) of the Charter.

While it is not simple to draw the line between further specifying the provisions of the law (e.g. as with adequacy decisions in Article 45 GDPR) and *applying* the law, it seems that Article 41a as proposed would be by far the closest to the *application* of the law (e.g. defining specific "*criteria*" or "*categories for controllers*"), which can increasingly infringe on the independence of supervisory authorities under Article 8(3) of the Charter and/or the role of the EDPB.

Furthermore, while Implementing Acts can legally be used for major decisions, they may not be a constitutionally suitable instrument to change the core definitions of a law that in turn implements a Fundamental Right.

See Article 4(1) GDPR above on the need to interpret the term "personal data" in line with Article 8 of the Charter, which in turn uses the definition of Directive 95/46.

Case Law

For the case law on the definition of "*personal data*" see Article 4(1) GDPR above.

Legal Certainty

Given the extremely unclear wording proposed for Article 4(1), it seems that Article 41a is intended to bring the necessary legal certainty to the definition.

However, the choice of an Implementing Act instead of a clear provision in the GDPR means that any change to the definition in an Implementing Act that goes beyond Article 4(1) GDPR or the CJEU's interpretation of "*personal data*" under Article 8 of the Charter could be subject to annulment procedures under Article 263 TFEU, with major implications for legal certainty:

- As can be seen from the EU-US data transfers saga, such legal challenges can bring massive legal uncertainty for controllers and processors.
- Any Annulment also has an *ex tunc* application, meaning that processing becomes illegal retroactively – opening up controllers to potential fines and claims for damages if they relied on any overly broad Implementing Act.

The text itself (see below) also provides for few safeguards as to the Commission's use of the provision.

Much of the legal certainty would therefore depend on the Commission's practical use of the powers under Article 41a.

The temporal aspects in relation to fast moving technologies may also generate legal uncertainty as an Implementing Act and the technological development may quickly deviate from each other:

- According to paragraph 2(a) of the proposal, the Commission may only "*assess the state of the art of available techniques*".
- This would mean that any definition may not assess the foreseeable development of tools that in the future would allow re-identification of data subjects.
- The assessment would therefore be largely "*backwards looking*", which is again not in line with CJEU case law, as certain processing is "*reasonably likely*" in the foreseeable future.
- Accounting for quick development of technology, the criteria for effective pseudonymisation that the act proposes may become obsolete quickly, as re-identification tools advance.
- At the same time the change of Implement Acts can take months or years from any initial realisation that a technical reality has changed. Based on this, entities might have a false sense of assurance that their processing is indeed compliant and that they cannot identify the individuals, whereas in reality tech advancements have already surpassed these assumptions.
- This is typically the reason why the GDPR took a technologically natural approach, with clear and strong general definitions, but without prescribing specific technical implementations.

Even if the Commission does a perfect job in drafting an Implementing Act, from the perspective of controllers or data subjects, the fact that according to Article 41a(3) the criteria in the Implementing Act should only be used as an "*element to demonstrate*" that Article 4(1) does not apply anymore would lead to massive legal uncertainty, because there would still need to be a case-by-case analysis.

Legal Quality

Despite the fact that European Parliament and Council have removed the many proposed options for Implementing Acts in the current GDPR, it seems that the Commission takes another attempt to gain more political leeway.

It is a highly questionable approach that the lacking legal quality of Article 4(1) GDPR should be "resolved" by allowing the Commission to define things further in an unknown, future act.

What can be said so far, is that Article 41a GDPR itself does not provide much more legal certainty:

- The commission would be allowed to specify technical and organisational ways ("*means*") but also additional "*criteria*" (likely beyond Article 4(1) GDPR) to determine if any processing would fall under the GDPR.
- This could be anything from inadequate means like "hashing" of an email to criteria about sizes of controllers or other elements to determine the "*likelihood*" that an identification may occur. There does not seem to be any real limitation, given that almost any objective or subjective element can be seen as a "*criteria*" in any legal instrument.
- The text does indicate that the "*category*" of "*controllers or recipients*" should play a role, which could hint at sectoral "*criteria*" to exclude entities from the GDPR.

In practice, the chosen approach would also mean that the Commission is almost entirely dependent on outside (usually private sector) input on available "*means*" and "*techniques*", given that the Commission will hardly develop such techniques itself and usually does not have sufficient technical expertise.

Conflicts

Articles 4(5), 11, 25 and 32 of the GDPR already provide a framework for identification and pseudonymisation.

The fact that the GDPR would now use the same word "*pseudonymous*" for data that may or may not fall under the GDPR seems very confusing:

- Article 4(5) GDPR clarifies that pseudonymous data is still personal data, while Article 41a GDPR allows for "*elements to demonstrate*" that this is not the case.
- Recital 26 of the GDPR states that personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person. Meaning, just because the entity currently does not possess the necessary information to identify an individual, it does not mean that the pseudonymised data is not personal data.
- While the new Recital 28 of the Omnibus states that the introduction of 'pseudonymisation' should not preclude any other measures of data protection, the exact opposite would not (partly) become true.

It is crucial to understand that in these Articles, where pseudonymisation is mentioned, it is always mentioned as a security measure or a data minimization measure, but this always requires logically that such data is still considered personal data.

It is unclear how the current Articles will interplay with the proposed Implementation Act, and if there will be conflicts, overlaps or ambiguities.

For more potential conflicts, please see the Conflicts section of the Article 4(1) analysis.

Simplification

While clearer "lists" would generally simplify the application of the law, the increased uncertainty introduced by Article 4(1) and the fact that Article 41b would only generate "*an element to demonstrate*" that a controller does not fall under the GDPR would probably make the overall application of the GDPR even more complex for SMEs and controllers without any deep understating of the GDPR.

After all it would still be a case-by-case assessment for any controller, with potentially € 20 million or 4% in a fine, if the controller made an inaccurate assessment, because e.g. the Implementing Act became technically outdated.

Data Subjects

See Article 4(1) GDPR above highlighting that data subjects are structurally unable to check or proof that elements in any Implementing Act under Article 41a were actually carried out properly.

The "chicken and egg" issue between the right to access (that is limited to "*personal data*") and the need to prove that it is actually "*personal data*" also applies with regards to Article 41a Implementing Act.

Controllers

See Article 4(1) GDPR above.

It is possible that situations similar to "regulatory arbitrage" might occur, where organisations invent structures that bypass the GDPR.

For example, instead of asking for further consent for additional processing, a company could outsource that processing to another entity who already has met the criteria under the implementation acts, and would thus not be covered by the GDPR.

Supervisory Authorities

See Article 4(1) GDPR above on the massive enforcement issues if supervisory authorities have to extensively research if a controller actually processed "*personal data*" in each case.

Harmonisation issues might occur since processing by some entities would be covered by the GDPR, while processing by others would not be.

This can create issues for the DPAs since they would have to interpret criteria differently in different cases. For example, confusion might arise if two parties process the same exact data, but only one of them has access (but does not use) to another database that allows for identification of a person. In this case, although the processing activities are identical, only one of the parties would be subject to the GDPR.

Real Life Examples

The litigation in *Schrems I* and *Schrems II* demonstrates the legal uncertainty that can be created if the Commission is coming under massive political pressure to make certain findings in Implementing Acts, which controllers rely upon, just to find out that the CJEU can overturn them with an *ex tunc* effect.

Article 88a - Access to Terminal Equipment

Proposed Text

(1) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation.

(2) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1)

(3) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following:

a) carrying out the transmission of an electronic communication over an electronic communications network;
b) providing a service explicitly requested by the data subject;
c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use;
d) maintaining or restoring the security of a controller's service requested by the data subject or the terminal equipment used for the provision of such service.

(4) Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply:

a) the data subject shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means
b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject;
c) if the data subject declines a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.

This paragraph also applies to the subsequent processing of personal data based on consent.

(5) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]

Proposed Recitals

(44) The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment and the subsequent processing of such data should be regulated under a single legal framework, namely Regulation (EU) 2016/679, where the subscriber of the electronic communications service or the user of the terminal equipment is a natural person. The amendments presented in this Regulation continue to offer the highest levels of protection for personal data, while simplifying the experiences of data subjects in exerting their rights and expressing their choices online. The amendments concern in particular storage of information in that equipment, accessing or otherwise collecting information from that equipment that entails the processing of personal data through cookies or similar technologies to gain information from the terminal equipment. The relevant rules should also apply regardless of whether the terminal equipment is owned by the natural person or by another legal or natural person.
The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment should continue to be allowed only on the basis of consent.

Similar to the approach in Directive 2002/58/EC, this requirement should not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, when that is based on Union or Member State law within the meaning of Article 6 of Regulation (EU) 2016/679 and if it fulfils all conditions of lawfulness laid down in that provision, and is done for the objectives laid down in Article 23(1) of Regulation (EU) 2016/679.
With a view to reducing the compliance burden and providing legal clarity to controllers, and given that certain purposes of processing pose a low risk to the rights and freedoms of data subjects or that such processing may be necessary to provide a service requested by the data subject, it is necessary to define a limitative list of purposes for which the processing should be permitted without consent. As regards storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment, and subsequent processing that is necessary for those purposes, this Regulation should therefore provide that the processing is lawful. The controller, such as a media service provider, may mandate a processor, such as a market research company, to carry out the processing on its behalf.
For the subsequent processing of personal data for other purpose than those defined in the limitative list, Article 6 and, where relevant, Article 9 of Regulation (EU) 2016/679 should be applied. It is the responsibility of the controller in the light of the principle of accountability to choose the appropriate legal basis for the intended processing. In order to be able to rely on legitimate interest under Article 6(1), point f, of Regulation (EU) 2016/679 as a ground for the subsequent processing of personal data, the controller must show that it pursues the controller's or third parties' legitimate interest, the processing is necessary in order to achieve the purpose of that legitimate interest, and the interests or fundamental rights of the data subject do not override the interests pursued by the controller. In this context, controllers should take outmost account of the following elements: whether the data subject is a child; the reasonable expectations of data subject; the impact on the individual either because of the scale of data processed or the sensitivity of the data processed; the scale of the processing at issue in the sense that the processing cannot be particularly extensive either because of their amount or the range of categories of data; the processing should be based on data limited to what is necessary and cannot be based on monitoring of large parts of the online activity of the data subjects; and other relevant factors as appropriate. The processing should not give rise to the continuous monitoring of the data subject's private life.
Where the controller cannot rely on legitimate interest as a legal ground for the subsequent processing, the processing should be based on another ground in Article 6(1), in particular on consent in accordance with Articles 6 and 7 of Regulation (EU) 2016/679, provided that all principles of Regulation (EU) 2016/679 are met.

(45) Data subjects that have refused a request for consent are often confronted with a new request to give consent each time they visit the same controller's online service again. This may have detrimental effects to the data subjects which may consent just in order to avoid repeating requests.The controller should therefore be obliged to respect the data subject's choices to refuse a request for consent for at least a certain period.

Overview

Together with the proposed changes to Article 5(3) ePrivacy Directive, the Commission proposes a distinction between the storage of and access to personal and non-personal data in a terminal equipment. It is therefore important to read this section in combination with the section on Article 5(3) ePrivacy Directive below.

This provision concerns the processing of personal data (in particular the storing and access) in the terminal equipment of natural persons. While this provision is meant to replace the commonly called the "cookie law", many other situations exist where data can be stored or retrieved from a terminal equipment. The law covers any technical access of personal data on a smartphone, PC, smart TV or IoT device. It is therefore concerned with controllers that are factually able to "pull" data from a device or store data in a device.

Article 88a functions as a *lex specialis* when processing (see Article 4(2) GDPR), consisting of "*access*" or "*storage*" on a "*terminal equipment*". Paragraphs 1, 2 and 3 relate to the at least 5 legal bases on which processing in the terminal equipment of natural persons can be made. It thereby seems to displace Article 6(1) GDPR when it comes to the "*access*" or "*storage*" on a "*terminal equipment*".

Paragraph 4 relates to deceptive design and so-called "dark patterns". It requires a "*single-click button*" which avoids issues such as consent buttons being hidden in a "second layer" or providing another type of interface than a "button" (e.g. just having a small link). Paragraph 5 relates to the entry into force.

Charter

Article 5(3) of the ePrivacy Directive aims at protecting the rights in Article 7 and 8 of the Charter (see Recital 2 of Directive 2002/58/EC).

Article 7 of the Charter protects, among other aspects, the communications of everyone, including legal persons. As messages or emails are typically stored locally on user devices, the provision offers certain protection against access to said communication.

From a Charter perspective, the fact that the proposal in Article 88a GDPR would allow more permissive access to devices for "*personal data*" than Article 5(3) ePrivacy allows for "*non-personal data*" seems hard to justify under Article 20 and 52(1) of the Charter.

Concerning the legal bases, consent is explicitly foreseen in Article 8(2) of the Charter, and the legislator can add another legal basis.

The Article 52(1) element of "*necessary*" is properly implemented in Article 88a(3) for all legal basis.

The legal basis under Article 88a(3)(a) a (b) may by their nature be understood as situations of "implicit consent", where (similar to Article 6(1)(b) GDPR) the legislator can assume that a data subject wishes the processing.

However, Article 88a(3) foresees two more "*absolute allowances*", which means that any necessary balancing under Article 52(1) of the Charter must already be done by the legislator (other than e.g. under Article 6(1)(f) GDPR, where this must be done when applying the law):

- Under Article 88a(3)(c) it seems conceivable that a proper balance is struck if personal data is instantly anonymised through aggregation and therefore the only processing allowed under this provision would be the short steps right before generating an aggregated number.
- Under Article 88a(3)(d) however it seems questionable if any interest in "*maintaining or restoring the security of a controller's service*" is in all cases overriding the fundamental rights of the data subject under Articles 7 and 8 of the Charter (see below for examples where this may not be the case).

In an initial analysis, it seems that Article 88a(3)(d) may go beyond what can be argues as being a "*proportionate*" limitation of the rights under Article 7 and 8 of the Charter.

Case Law

As the article is new, there is no case law directly concerning it.

Even if called differently, a requirement for "one-click button" to reject consent requests is in line with current case law.

At the same time, the "one-click button" requirement falls behind most current guidelines and case law of supervisory authorities on "dark patterns" used in consent banners. Many supervisory authorities developed much more comprehensive rules on design, colors or deceptive wording – which will continue to apply.

Legal Certainty

The following section is separated by elements of Article 88a.

The fact that rather clear (see for specific problems below) situations are explicitly legalised, with relevant limitations, seems to overall dramatically clarify the legal situation.

For many elements like consent or the use for transmission, it seems that legal certainty is achieved through a massive body of case law and the existing experience under Article 5(3) ePrivacy. We therefore focus on potentially problematic elements:

In relation to the wording "*terminal equipment of a natural person*" and "*that person*":

- It seems obvious that many devices are not

necessarily attributed solely to one person (e.g. a smart TV used by an entire family or a tablet used by a couple), nevertheless data placed on the device is regally "*personal data*", as it links to a personal account or alike.
- The text may also lead to confusion around corporate devices, where it can be disputed if a corporate laptop that is in practice exclusive used by one employee is an "*equipment of a natural person*" or the equipment of the employer.
- The linking to an individual is already (in most cases) achieved through the reference to "personal data". Adding a second link to an individual in the definition seems to create increased confusion.

On the allowance for common website statistics, it seems that the combined elements to scope the provision ("*aggregated information*", "*usage of an online service*") and the limitation in purposes ("*to measure the audience*" or "*solely for its own use*") and possible parties ("*by the controller*") make the scope sufficiently clear. It may warrant clarification if "*by the controller*" would exclude the use of a processor under the authority of the controller, which would exclude the common practice of having a hosting provider or third-party statistics provider. The risk of "secondary use" by a third party like Google Analytics should already be captured by the wording "*solely for its own use*".

With regards to "*maintaining the security of a service*":

- It must be noted that this can be very broad and can allow broad and massive searching of locally stored data on smart phones, PCs and alike (towards a "remote search" of devices).
- This could entail unintended consequences similar to the discussions about "upload filters" and alike.
- Article 88a could in this regard be read to allow overly invasive techniques on user devices - which would in turn go far beyond anything that would likely be accepted by the CJEU under Articles 7 and 8 of the Charter.
- So far, processing for security purposes would often be discussed under Article 6(1)(f) GDPR, which requires the tree step tests (security being generally a legitimate interest, but controllers may not be able to demonstrate that such massive search is indeed "*necessary*" and especially not "*proportionate*").
- Such a test seems to be missing in Article 88a(3)(d), which could in turn require the factual addition of such a test when interpreting the provision "*in light of the Charter*", which would create additional legal uncertainty.

With regards to Article 88a(4), the lack of a tech neutral wording could lead to unclear situations:

- Only requiring a "*one-click button*" would not fit to situations where other interfaces than buttons (e.g. toggles, swipes, voice control) are used by a controller.
- The addition of "*equivalent means*" on the other hand could be interpreted by controllers that there is free choice ("*or*") between a single-click button and e.g. a tiny link to reject consent.
- Overall, the wording could be improved. By comparison Article 7(4) GDPR ("*It shall be as easy to withdraw as to give consent.*") seems to regulate a similar matter in a tech neutral way and without any option for (intentional) misunderstandings.

Legal Quality

Overall, there seem to be no massive legal quality issued beyond elements mentioned in other sections above and below.

The narrative of a "single-click button" approach may be easy to explain to the general public or the media. However, from a purely legal perspective a simple addition to the existing Article 7(3) along the lines of "*It shall be as easy to [reject and] withdraw as to give consent*" would have been clearly more elegant and would have been in line with the GDPR typical "tech neutral" approach.

It is also unfortunate that the Commission proposal does not take the occasion to explicitly regulate very common other dark patterns in consent banners and also expands the ban on ridiculous reject options (e.g. "*strike through this section*" in contracts) in offline contexts.

Article 88a(2) seem to overlap largely with the function of Article 23 GDPR. It seems more consistent to add a reference in Article 23 to Article 88a, instead of the opposite direction.

Conflicts

The logical conflict between Article 5(3) ePrivacy and Article 88a GDPR, which leads to a more protective situation for "*non-personal data*" (see above) is not explainable.

The interplay with Article 5(3) ePrivacy could also lead to gaps or situations where both regimes apply (see comments on Article 5(3) on the interplay with this article).

Other legal instruments (e.g. DMA or ePrivacy) increasingly refer to "*consent*" in the GDPR. Moreover, there are multiple "consent" options in the GDPR. Obviously, the "dark pattern" issue is also relevant for all these provisions. It is inconsistent that only Article 88a now foresees the "one-click" option. For example:

- The current wording would mean that "consent" for non-personal cookies (under the new Art 5(3) ePrivacy, that only refers to the definition of "consent" in Art 4(7) GDPR) would not require a "one click", but personal data would require such a "one click".
- It would also be illogical to only have a "one click" requirement for "normal" personal data, but not for Article 9 data or automated decisions under Article 22.

Again, the higher risk processing would then have less protection (as with other proposed changes).

Certain parts of Article 88a conflict with other articles or principles under the GDPR. For example, "security" is generally accepted to be a "legitimate interest" under Article 6(1)(f) GDPR, but requires a balancing test. The new provision (d) does not need such a balancing test, which may be problematic, because controllers could engage in unlimited processing for the tiniest of security reasons.

Simplification

The provision seems to simplify the matter of cookie banners in the following substantive ways:

- Most websites do not engage in online advertisement or tracking, but need a consent banner to be able to run (anonymous) statistics. Making this processing operation generally legal should ensure that cookie banners are gone on most "normal" websites in Europe.
- The "one-click button" is a partial simplification, however other deceptive designs are not mentioned and some of the pain of cookie banners may just move to patterns that are not about the existence of a reject button.

Data Subjects

We generally see a massive improvement for most data subject under Article 88a in combination with Article 88b of the proposal, that could overcome the public outrage about "consent banners".

At the same time issues mentioned above (e.g. access for security purposes) need a solution.

Controllers

The vast majority of controllers would massively benefit from Article 88a(3), not just because of more limited compliance costs, but also because consent banners can increase "bounce rates" on commercial websites.

As explained, the text suggests that consent may not be repeated within 6 months. Controllers and processors will therefore have to find means to keep track of users choices. This can however be done e.g. with an anonymous "frequence capping" cookie. Questions remain about the need for consent for such a "already_asked" cookie under Article 5(3) ePrivacy.

Supervisory Authorities

In Member States where enforcement of Article 5(3) ePrivacy is not done by the GDPR supervisory authorities, there were already existing problems to coordinate cases.

The proposed approach to Articles 88a and 5(3) would now mean that in each case, the authorities would have to first investigate if "personal data" is concerned (which is often disputed by controllers) to then find out which authority is in charge of enforcement – either under Article 88a GDPR or 5(3) ePrivacy.

This enforcement split should have been overcome in order to streamline compliance, now the procedural overhead resulting from this "split" may even increase.

In international cases the problem may even increase, given that ePrivacy does not foresee a system to determine "*main establishments*" and the cooperation system in Article 60 to 66 GDPR is not available.

Real Life Examples

On the access to terminal data for security purposes:

- For example, video game companies scan the entire PC of gamers to ensure that players did not install "cheating" software. It seems questionable if such wide-spread scanning is indeed proportionate.
- Under the "Chat Control" discussion, the contents of communication (and potentially devices) would be scanned for security reasons.
- Producers of operating systems or hardware regularly transfer data from devices for security purposes. It seems that such transfers could be limited to users that consent to the processing, given that security problems usually concern large numbers of users, and software producers may only need a sufficient number of reports.

On the cooperation between GDPR supervisory authorities and telco regulators:

- In many Member States (e.g. Austria, Sweden, Slovakia, Finland or Norway) the telco regulator and the supervisory authority have overlapping competences for "cookies". In some Member States they sequence investigations (leading to even longer procedures) in other Member States they investigate the same matter largely in parallel, leading to conflicting decisions.

Article 88b - Automated Signals

Proposed Text

1. Controllers shall ensure that their online interfaces allow data subjects to:

(a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;
(b) decline a request for consent and exercise the right to object pursuant to Article 21(2) through automated and machine-readable means.

2. Controllers shall respect the choices made by data subjects in accordance with paragraph 1.

3. Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service.

4. The Commission shall, in accordance with Article 10(1) of Regulation (EU) 1025/2012, request one or more European standardisation organisations to draft standards for the interpretation of machine-readable indications of data subjects' choices.

Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 1.

5. Paragraphs 1 and 2 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation].

6. Providers of web browsers, which are not SMEs, shall provide the technical means to allow data subjects to give their consent and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to 5 of this Article.

7. Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation].

Proposed Recitals

(46) Data subjects should have the possibility to rely on automated and machine-readable indications of their choice to consent or refuse a consent request or object to the processing of data. Such means should follow the state of the art. They can be implemented in the settings of a web browser or in the EU Digital Identity Wallet as set out by Regulation (EU) 914/2014, or any other adequate means. Rules set out in this Regulation should support the emergence of market-driven solutions with appropriate interfaces. The controller should be obliged to respect automated and machine-readable indications of data subject's choices once there are available standards. In light of the importance of independent journalism in a democratic society and in order not to undermine the economic basis for that, media service providers should not be obliged to respect the machine-readable indications of data subject's choices. The obligation for providers of web browsers to provide the technical means for data subjects to make choices with respect to the processing should not undermine the possibility for media service providers to request consent by data subjects.

Overview

The replacement of consent banners ("cookie banners") with technological solutions that can be used to automatically inform about the user's privacy choises is about 20 years in the making. Previous efforts like "Do Not Track" (DNT) failed to become an official technical specification in the W3C and remained at draft status. In the US the "Global Privacy Control" (GPC) tool has been implemented recently. The idea of such signals is to communicate privacy preferences digitally, just like browser signals' language settings or screen resolution.

The US approach to such signals is based on a single opt-out setting in a browser, that is communicated to all websites. This clashes with the EU approach of specific, opt-in consent and the desire to have different settings per controller. Any EU signal would have to be able to communicate these dimensions to comply with Article 6(1)(a) GDPR and Article 8(2) of the Charter. *noyb* and the University for Economics in Vienna have provided a prototype of such a solution as "ADPC".

A *de facto* standard (the IAB's TCF) to signal choices between controllers exist already today. We welcome that the proposal aims to ensure that the "last mile" to the consumer would also be automated.

The provision can be separated in paragraphs 1 to 3 defining a duty of controllers to accept a digital choice signal (with an exemption for media service providers), paragraph 4 dealing with standardization of the signals and paragraphs 6 and 7 regarding the duty of web browsers to implement the functionality to send such a signal.

Charter

Already Article 8(2) of the Charter requires that processing is taking place for a specified purpose (e.g. advertisement, personalized content). Consent is not further defined but generally requires that the data subject is aware of the controller, relevant data and purposes.

The fact that "*media service providers*" are exempt from the duty to accept a signal may be challenging from an "equality before the law" principle perspective – see Article 20 of the Charter.

Case Law

There is no relevant case law to our knowledge specifically on privacy signals.

There is generally (national) case law that if a data subject uses a technical solution to generate legal declarations, they are liable for any false or unintentional communication. Such matters go back to faulty fax machines and the like. This can be used to ensure that controllers do not have to consider whether a signal truly represents an unambiguous action by a data subject.

Legal Certainty

The proposal provides almost no definitions as to the exact format of the signal (e.g. one general opt-out like DNT or GPC or a nuanced per controller / per purpose signal like ACPD). This could lead to massive disputes during the creation of the technical specifications.

The provision thereby also largely "outsources" crucial decisions with an impact on fundamental rights to technical standardisation bodies. Previous experiences with technical specifications have shown that industry groups heavily dominate such processes. The technical specification of DNT was even derailed by industry disagreement and failed. It is therefore advisable to include minimum requirements for the automated signal in the text of the law.

The newly added definitions in Article 4 (35) of "media service providers" and (36) "media service" (as in Article 2(1) and (2) of Regulation (EU) 2024/1083) seems to provide legal certainty as to who should be exempted from accepting user choices through automated means.

Legal Quality

Article 21(5) GDPR so far foresees a duty to allow an automated objection "*in the context of the use of information society services*". It is not clear in which contexts the provision applies:

- The new provision does not seem limited to certain contexts (e.g. web, mobile, IoT), but uses the term "online interfaces". The term is defined in Article 3(m) Digital Services Act as: "*any software, including a website or a part thereof, and applications, including mobile applications*".
- However, paragraph 6 of the proposed Article 88b would only provide a duty to be able to send such a signal from a browser, which would exclude the duty to have settings in mobile or PC operating systems for all applications running in these environments.

It is also unclear why only consent under Article 4(11) GDPR, the right to object under Article 21(2) GDPR and the (new) notion of "declining a request" is covered by Article 88b, but not the withdrawal of consent under Article 7(3) GDPR, when the law requires that "*it shall be as easy to withdraw as to give consent*."

Conflicts

Under the proposed definition of "personal data" in Article 4(1) GDPR, this solution may be limited to fewer and fewer situations.

It is unclear to what extent the remaining "non-personal data" provision in Article 5(3) of ePrivacy is covered by this signal. If it is not covered, users would still see a cookie banner only for non-personal data.

There is an increase in other EU laws that refer to Article 6(1)(a) GDPR for consent. It is unclear how these references would interact with the new requirements in Article 88b.

It seems Article 21(5) GDPR could be deleted to make the law consistent.

Simplification

The simplification for transactions between data subjects and controllers is obvious.

Most websites either (1) use a simple cookie banner that comes with the content management system (e.g. Wordpress) or (2) a dedicated "Consent Management Platform" ("CMP") to manage cookies. This means that just a handful of software providers need to implement a digital signal to make this technology available throughout the EU.

Equally on the user side, there is a small number of software providers for browsers and the like that regularly update their software and can easily implement such a functionality.

Data Subjects

For data subjects a signal is a major improvement that can overcome "consent fatigue" (which is mainly triggered by interfaces provided by controllers), but also allow data subjects to have more genuine choices by using certain settings instead of being confronted with ten thousands choices (given that one banner can have more than 1000 settings) per day.

However, the power of the interface may just be transferred to the browser manufacturers, a sector currently dominated by Google. It should therefore be considered to require that browsers allow third party management software (usually in the form of plugins) to take the role of consent management on the user side.

Controllers

Controllers will likely benefit from less "friction" on their website, because traditional cookie banners increase the "bounce rate", meaning people that just leave the website or service before interacting with it.

Controllers who push for higher consent rates via "dark patterns" will have significantly less opportunities to do so and supervisory authorities who have already pushed back on

such “dark patterns” will have less work with enforcing against such illegal behaviour.

The fact that media service providers are exempt could backfire, as only media pages would continue to show a “consent banner”, which has a massive warning function and could indicate to users that their personal data is more at risk on media pages than other websites. However, media companies could obviously still switch to voluntarily accepting a signal to overcome this problem.

The lack of a clear definition of contexts in which the law applies may also be hard to navigate for controllers. If a user interacts with a company on an app, via the mobile browser or a PC browser, the signal may only be available in one context and conflicting messages could be sent. If the scope of the application of such a signal is clarified (e.g. limited to the relevant context), such problems could be avoided.

Supervisory Authorities

The change could eliminate the “cookie banner” discussion to a large extent and limit the need for enforcement on the interfaces.

The actual treatment of a signal must however still be enforced. However, given that this is (largely) in the hand of a small number of software providers, we would assume that this would make enforcement simpler.

Real Life Examples

- “Do not Track” was massively delayed for years, because industry came up with more and more “problems” that needed to be taken care of. In the end standardization was abandoned.
- “Global Privacy Control” and DNT have a binary approach (yes/no) for all controllers and cannot communicate an opt-in, but only an opt-out. It is also not possible to communicate different purposes, as necessary under the GDPR (see guidelines of the EDPB on consent, p. 12).
- “Advanced Data Protection Control” is a standard for communication of users’ privacy choices that follows EU principles of consent (opt-in) and purpose-based consent on a per-controller basis.
- In France TCF signals (which is a B2B signal) were in certain cases manipulated, showing the need for precise technical specification and the need to be able to prove compliance in a technical standard.

Article 88c - AI Systems

Proposed Text

Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.

Proposed Recitals

(30) Trustworthy AI is key in providing for economic growth and supporting innovation with socially beneficial outcomes. The development and use of AI systems and the underlying models such as large language models and generative video models rely on data, including personal data, in various phases in the AI lifecycle, such as the training, testing and validation phase and may in some instances be retained in the AI system or the AI model. The processing of personal data in this context may therefore be carried out for purposes of a legitimate interest within the meaning of Article 6 of Regulation (EU) 2016/679, where appropriate. This does not affect the obligation of the controller to ensure that the development or use (deployment) of AI in a specific context or for specific purposes complies with other Union or national law, or to ensure compliance where its use is explicitly prohibited by law. It also does not affect its obligation to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.

(31) When the controller, in the light of the risk-based approach which informs the scalability of the obligations under this Regulation, is balancing the legitimate interest pursued by the controller or a third party and the interests, rights and freedoms of the data subject, consideration should be given to whether the interest pursued by the controller is beneficial for the data subject and society at large, which may for instance be the case where the processing of personal data is necessary for detecting and removing bias, thereby protecting data subjects from discrimination, or where the processing of personal data is aiming at ensuring accurate and safe outputs for a beneficial use, such as to improve accessibility to certain services. Consideration should also, among others, be given to reasonable expectations of the data subject based on their relationship with the controller, appropriate safeguards to minimise the impact on data subjects' rights such as providing enhanced transparency to data subjects, providing an unconditional right to object to the processing of their personal data, respecting technical indications embedded in a service limiting the use of data for AI development by third parties, the use of other state of the art privacy preserving techniques for AI training and appropriate technical measures to effectively minimise risks resulting, for example, from regurgitation, data leakage and other intended no foreseeable actions.

Overview

The original arguments in the 1980ies to introduce principles like transparency, accuracy, data minimisation, purpose limitation and alike were the risks of the foreseeable future, where untransparent algorithms would use the personal data of everyone and produce unforeseeable results that impact peoples' lives. Many of these descriptions correspond exactly to what happens today with "AI". It is therefore not surprising, that AI development and deployment is restricted by the very rules that were written to limit unintended consequences from such systems. Any changes to the GDPR must be seen with the original intention of the law in mind.

At the core of the debate on AI training is the need to either collect consent from sufficient users to be able to train data (opt-in) or to allow companies to just use everyone's data and merely allow an objection (opt-out). The Commission proposal goes towards shifting the burden of micromanaging user choices to 450 million Europeans – instead of a handful of AI training companies.

The proposed article codifies the possibility to rely on legitimate interest under Article 6(1)(f) GDPR as a legal basis to develop and operate AI systems, but still requires "*necessity*" and a multi-factor test ("*balancing*") as for any other processing under Article 6(1)(f) GDPR. The provision adds the requirement of "enhanced transparency" and an unconditional opt-out, in line with Article 21(2) GDPR. Overall Article 88c acts as a *lex specials* version of Article 6(1)(f) GDPR.

Just like the proposed Article 9(2)(k) and (5), this provision provides an allowance for controllers to process personal data for the development and operation of AI systems and models. The proposed provision uses enigmatic language ("*may be pursued*", "*where appropriate*", "*appropriate* [...] *measures and safeguards*").

In addition, the Commission suggests some organisational, technical measures and safeguards which are presented as examples and not as an exhaustive list, giving leeway to controllers to assess what is in their view "*appropriate*".

The proposed article seems to overall favour AI applications over any other technical approaches to data processing (e.g. a normal database), which would not benefit from having a "*legitimate interest*" codified in law. The provision therefore leaves the "tech neutral" approach of the GDPR and generates a favourable rule for only one technology.

Charter

See details under Article 9(2)(k) and 9(5) GDPR for the assessment of the proposed AI exemptions under the Charter.

Case Law

So far, broad scraping of data (that included incidental personal data) merely for a commercial interest was not seen as complying with Article 6(1)(f) GDPR, the Commission therefore departs from the current case law to a certain extent:

- In C-131/12, *Google Spain*, §81 the CJEU already recognised the dangers associated with broad internet scraping and considered that mere commercial purpose is not a legitimate interest to scrape the internet, but that access to information for the users of a search engine can overcome the rights of individuals under Art 6(1)(f) in light of Article 11 of the Charter (right to information). However, measures like delisting ("*right to be forgotten*") were required.

The Commission now proposes to introduce a co-called "legal fiction" that a legitimate interest always exists in the case of development and operation of AI systems. However, such a legal fiction cannot overcome many other requirements to rely on Article 6(1)(f) GDPR in the logic of Article 6(1)(f) GDPR and the case law:

- In C-621/22, *Tennisbond*, § 49 it was held that to rely on legitimate interest, the controller must comply with all of its obligations under

the GDPR, including the transparency obligations.
– In C-252/21 *Bundeskartellamt*, §67, the CJEU specifies that this information should include the legal basis for the processing and the precise legitimate interest. In §107 of the same decision, the CJEU also specified that the information must be given to the data subject at the time of the collection of the personal data.

This can lead to interesting results in relation to AI training. For example: The Italian Supervisory Authority has ordered OpenAI to inform people about the training via a "*public awareness campaign*", effectively buying TV ads, billboards and alike.

Furthermore, the interpretation of the necessity requirement of the three-step test under Article 6(1)(f), which according to the new provision still needs to take place according to the proposed Article 88c as well, is strict according to the CJEU and will likely clash with the Commission's take on the necessity of the processing of personal data for the development and operation of AI systems or models.

– In C-621/22 *Tennisbond* § 51, the CJEU set a strict interpretation for the necessity criterion: it considered that a sport club sending members data to third parties for advertising purposes did not fulfil the necessity requirement as it should have informed the members beforehand and ask them whether they wanted their data to be transmitted with the third parties. The same reasoning should be applied and would likely lead to non-fulfilment of the necessity test in the context of the application of Article 88c;

The correct and logical CJEU case law requires to also take into account violations of principles in Article 5(1) or the rights of data subjects, for example when data cannot be corrected or deleted, or access to data in an AI system cannot be provided, when doing the "balancing" in the tree-step test.

The Commission proposal does not address this obvious conflict between the approaches of many current AI developers and the law.

Legal Certainty

On the scope of the provision:

– The wording "*in the context of*" is extremely broad and makes it very unclear when Article 88c and when Article 6(1)(f) would govern the processing. Similar wording in Article 3(1), 4(16)(b) or 4(23) GDPR were read in an extensive way and regularly led to disputes about the scope of said definitions.
– The inclusion of "operation" would lead to massive illogical consequences, such as that processing via an AI System would be preferable since it would count as a "legitimate interest" by default, while processing via another system (e.g. a normal database or in an Excel sheet) would by default not be a "legitimate interest".
– The reference to Article 3(l) of the AI Act leads to another, expansive application of Article 88c, given that the definition of AI systems is extremely broad in the AI Act. Many "*normal*" processing activities would then suddenly fall under Article 88c, which would e.g. trigger the legal fiction of a "*legitimate interest*", but also the absolute opt-out or the need for "*enhanced transparency*" in areas that were not meant to be covered.

The proposal provides that controllers can rely on their legitimate interest "*where appropriate*", seemingly adding another requirement to the legitimate interest assessment, without clarifying what would pass this new test of "*appropriateness*" according to the GDPR. This phrase does not add any clarity on the existing legitimate interest assessment that the controllers need to conduct nor does it provide legal certainty over a highly disputed processing operation.

Legal Quality

The proposed provision uses extensive enigmatic language ("*may be pursued*", "*where appropriate*", "*appropriate* [...] *measures and safeguards*") which is partly taken from other Articles of the GDPR (where they have proven to be hard to apply) or raise questions as to their operative meaning. The proposed safegards are worded as examples ("*such as*") and are not an

exhaustive list, which is likely going to cause more confusion than clarity.

So far Article 6(1) is "*technologically neutral*". In the Commission's proposal a specific technology (not a purpose or processing aim!) is for the first time (somehow) legitimised.

This may also mean that processing is only legal, because AI is used – while it would otherwise not fall under Article 6(1) GDPR. The provision could impair the tech neutrality of the GDPR and imply that new technologies also raise debate and need specific provision.

Conflicts

There is a bigger "slippery slope" and consistency issue that Article 88c raises. If legitimate interest is found for "*scraping the entire internet*" and any other available training data, for basically commercial purposes (AI companies currently have evaluations of trillions), there is little other processing that would not be a "legitimate interest". See the comparison with the *Google Spain* ruling above.

Given that controllers may not have any direct contact with data subjects and data subjects may never have heard of a specific controller it is entirely unclear how the "*unconditional right to object*" should be implemented in practice:

- Data subjects would have to be made aware of the fact that (1) they are in a training data set (which is largely kept secret as "business secrets" and alike), that (2) a controller is about to use that data set for training and (3) what time-frame applies to the objection.
- Controllers on the other hand would have to (1) identify individuals in a data set, (2) find their contact details, (3) allow the opt-out via any form of communication according to Article 12 GDPR and (4) then find the relevant data to be removed.
- Moreover, the right to object is an *ex post* right, that can be exercised at any time. The draft does not seem to address that, meaning that data subjects could "opt out" after the training has already started.

While being fully aware that Article 88c will hardly be acceptable under Article 8 of the Charter without information and a right to object, it seems that the provision is so far not really ready for practice beyond Big Tech platforms that use personal data from a (somewhat) structured source and have a direct contact with data subjects.

There are further inconsistencies with the current approach of AI training companies and the GDPR, that Article 88c does not resolve. To name a few:

- According to Recital 47, "*the interests and fundamental rights of the data subject may in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect such processing*". The new Recital 31 repeats that. In case of AI training and operation, the complexity, multiplicity and constant evolution of the systems imply that data subjects can neither reasonably expect that the processing of their data takes place nor the extent of the processing.
- The new wording also ignores that the relevant time period that is taken into account for the assessment of the reasonable expectations of the data subject is at the time of the collection of the data. For social media and controllers such as big tech companies which have been around for decades, the reasonable expectation should be considered from the starting point of the contractual relationship (e.g. for Facebook).

The proposal provides that controllers can train and operate AI systems or models according to Article 6(1)(f) GDPR except where consent is explicitly required by Union or Member State law. According to the Commission's Staff Working Document (p. 39) accompanying the proposal, this phrase was added to reflect the requirements for consent that the gatekeepers have to respect under the Digital Markets Act. However, this wording also includes a national option: Member States that might be opposed to processing AI training and operation with users' personal data under legitimate interest could introduce a consent requirement. This could obviously lead to a fragmentation of the Digital Single Market.

Simplification

The Commission's proposal does not seem to simplify or solve the question whether controllers can rely on legitimate interest for AI training, but largely just copies Article 6(1)(f) GDPR.

The additional elements in the provision (e.g. undefined safeguards) do not seem to make the application of Article 88c GDPR any simpler.

In other words: the problem with AI training was not to agree that it may (!) be a legitimate interest, but the fulfilment of the necessity and the balancing test. Both steps of the Article 6(1)(f) test are not materially clarified by Article 88c.

From a data subjects' perspective opting out from hundreds or thousands of controllers' AI systems does also not seem like a simplification.

Data Subjects

The proposed text will likely send a political signal that AI training and operation is generally legal, even if the legal wording still requires a balancing test. For data subjects it is notoriously difficult to challenge the balancing test under Article 6(1)(f) GDPR because controllers do not have to publish the details.

The enforcement of key rights by the data subject (e.g. access, rectification or deletion) likely continues to be a problem in reality.

Furthermore, even if the "*unconditional objection*" is successfully implemented data subjects would have to "object" to hundreds or even thousands of controllers per year, making this protection basically not manageable for data subjects. There are options (e.g. central "Robinson List" for central lists for direct marketing opt-outs) to at least make the "opt out" workable in practice, but the current draft does not seem to take these experiences into account.

Controllers

A massive practical problem is that AI training and processing may use more "messy" and "unstructured" data than other systems. This makes many of the "safeguards" that are proposed impossible or at least impracticable in practice:

- Usually, controllers do not have contact details or even just a direct relationship with the data subject.
- Equally, data subjects may not know about the (ever increasing) number of controllers that scrape publicly available data that contains their details. Lacking such awareness, they cannot exercise their rights or get relevant information.
- Finally, controllers will often be unable to accurately find personal data in unstructured data, without massive investment in manual labour (that they traditionally reject considering).

Supervisory Authorities

Supervisory authorities will be called to interpret the proposed provisions, enforce accurate balancing under Article 88c, compliance with opt-outs and (undefined) "*safeguards*".

Given the fact that most supervisory authorities are overburdened and their resources are very limited, they will likely be unable examine the technical and organisational measures of AI applications with limited available expertise and barely existing case law at hand.

Furthermore, the broad definition of "AI" and the fact that the mere operation of an "AI" system would fall under Article 88c could mean that many situations where supervisory authorities have established case law and compliance procedures would have to be reassessed under Article 88c once "AI" is used for the exact same processing purpose as some previous "normal" database or software.

This could lead to a growing factual departure from any compliance with the GDPR.

Real Life Examples

noyb has an increasing number of complaints on AI systems that

- Basically, all AI systems clearly allow to reproduce personal data about individuals, which means that training data is openly available to any user.
- There is an increasing number of persistently false results in relation to normal persons in AI chat systems, such as people being accused of murdering children. AI companies largely ignore the right to rectification or deletion in such cases.
- Almost all social networks (e.g. Twitter, LinkedIn, Facebook, Instagram) have by now decided to engage in "secondary use" of all available personal data for AI training. Partly it is openly said, that "opt outs" are not fully functioning (e.g. if a person is in pictures uploaded by other people).
- Many other companies with access to personal data (e.g. Google or Microsoft) have also announced to use data that they may hold as processor or for other purposes for AI training. In some cases, these projects are not yet using EU/EEA data, but there is an increasing trend towards absolutely ignoring the red lines of the GDPR, such as Article 5(1)(b) or Article 28 GDPR.

Overall we see a massive "theft" of personal data from other controllers and data subjects to train an operate AI systems, that enrich a small number of companies – which in turn are valued at Trillions (!) of Euros, based on data, intellectual work and knowledge that the rest of society has produced.

Article 5(3) ePrivacy

Current Text

(3) Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

Proposed Text

(3) Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

This paragraph shall not apply if the subscriber or user is a natural person, and the information stored or accessed constitutes or leads to the processing of personal data.

Proposed Recitals

(47) Directive 2002/58/EC on privacy and electronic communications 'ePrivacy Directive'), last revised in 2009, provides a framework for the protection of the right to privacy, including the confidentiality of communications. It also specifies Regulation (EU) 2016/679 in relation to processing of personal data in the context of electronic communication services. It protects the privacy and the integrity of user's or subscriber's terminal equipment used for such communications. The current provision of Article 5(3) of Directive 2002/58/EC should remain applicable insofar as the subscriber or user is not a natural person, and the information stored or accessed does not constitute or lead to the processing of personal data.

Overview

Together with the proposed changes to Article 88a GDPR, the Commission proposes a distinction between the storage and access to personal and non-personal data in a terminal equipment. It is therefore important to read this section in combination with the section in Article 88a GDPR.

The provision in Article 5(3) ePrivacy Directive was created to limit access to devices (either by storing or accessing information on the device), independently of the nature of the information. This seeks to ensure "device integrity" based on Article 7 and 8 of the Charter.

The law covers any technical access of personal data on a smartphone, PC, smart TV or IoT device. It is therefore concerned with controllers that are factually able to "pull" data from a device or store data in a device, not merely with the placement of "cookies".

Under the current regime, when personal data is at stake, the provision operates as a *lex specialis*, taking precedence over the GDPR or other rules for installing or accessing data on a device.

The proposed changes would do away with the previous logic of this provision and how it interacted with the GDPR. This would change the regime for the protection of personal data on devices as currently provided by Article 5(3) ePrivacy Directive and would lead to the application of the more permissive and newly proposed Article 88a GDPR for personal data, while the current (more restrictive) approach is maintained for access to non-personal data.

Charter

Article 7 of the Charter protects, among other aspects, privacy in communications. As emails and many messages are commonly stored on user devices, the provision offers certain protection against access to said communication. Article 7 of the Charter is also not limited to natural persons – businesses can be an aim as well when privacy in communication is undermined.

For the issues that may results from the interplay of Article 5(3) ePrivacy and Article 88a GDPR from the perspective of the Charter (primarily potential violations of Article 20 and 52(1) of the Charter) see above the relevant section on Article 88a.

Case Law

There is naturally no relevant case law in relation to the newly introduced provision on the interplay of Articles 88a and 5(3).

Legal Certainty

The fact that the we would now have two legal regimes in Article 5(3) ePrivacy and Article 88c GDPR that are similar, but different (different legal basis, etc) is inherently confusing.

Plus, the difference hinges on the (potentially more obscure) definition of "*personal data*" in an amended Article 4(1) and 41a GDPR, adding to the confusion.

Legal Quality

The wording "*constitutes or leads to the processing of personal data*" is unclear and it is undefined what would be understood as "leading" to processing personal data.

In combination with Article 88a GDPR that only applied to the "*processing*" of personal data, there would be a gap where data that "*leads to the processing*" is neither covered by Article 5(3) ePrivacy nor by Article 88a GDPR.

Conflicts

The rules for non-personal data will be stricter than for personal data (see above).

The more permissive rules under Article 88a GDPR could lead to controllers aiming at processing "*personal data*" in order to benefit from the less restrictive provisions in the GDPR. This is contrary to the principle of processing data only where it is necessary and potentially creates a wrong incentive.

Simplification

There seems to be no simplification, given that two similar but different legal regimes remain and the separation between them (so far, the act of accessing or retrieving information, versus processing personal data) was replaced with a separation between personal and non-personal data, which is increasingly unclear in the light of the proposed changes in Articles 4(1) and 41b GDPR.

Furthermore, the improvements around consent banners in Article 88a and 88b do not seem to link to Article 5(3) ePrivacy, meaning that even if a browser signal and a "single-click button" is required by the GDPR, any placement of non-personal data would still fall under the current regime.

Data Subjects

See the comments under Article 88a above.

Data subjects will, even more than online service providers, struggle to know if the provision in Article 5(3) ePrivacy Directive (or the corresponding national law) applies to them.

It will become even more unclear to data subjects which enforcement authority to contact, in case they consider their rights infringed – creating even more delays in enforcement.

Controllers

See the comments under Article 88a above.

The difference between Article 88a GDPR and Article 5(3) ePrivacy will likely generate additional overhead and regulatory complexity for controllers.

Supervisory Authorities

See the comments under Article 88a above on the increased complexity to determine the responsibility for online tracking between Supervisory Authorities and other regulators, such as telecoms regulators.

Imprint:
noyb – European Center for Digital Rights

Goldschlagstraße 172/4/3/2
1140 Vienna

ZVR: 1354838270