Notes:

- Left side is actual text, right side is the new text;
- ~~crossed out~~ - means deleted in the original;
- **bold** - means added to the original;
- regular – is the original, unchanged text.
- Gray Highlight – especially crucial elements, added by *noyb*.

GDPR		
Recital without connection to a specific new Article: (36) Regulation (EU) 2018/1725 of the European Parliament and of the Council applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Directive (EU) 2016/680 of the European Parliament and of the Council applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Regulation (EU) 2018/1725 and the Directive (EU) 2016/680 should be aligned with the applicable amendments to the Regulation (EU) 2016/679 established by this Regulation. In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Regulation (EU) 2018/1725, Directive (EU) 2016/680 and any other Union legal act applicable to such processing of personal data should follow after the adoption of this Regulation, in order to allow for their application as close as possible to the entry into application of the amendments to Regulation (EU) 2016/679.		
Article 4 - Definitions		
Current version	**Proposed version**	**Comments**
(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;	(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.	**Note: See below Article 41a** for the option of further definitions by the Commission. The change attempts to include the "relative" approach to personal data under C-413/23 P EDPS v SRB, but seems to go further than that, or at least codify (only) the expansive elements of that judgement.

Current Recital: (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 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.	**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 subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.** **Connected New Recital:** (25) 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	The limitations on "personal data" are: **(1)** a **highly "subjective" approach** per controller to define if the GDPR even applies to a processing activity, versus an "objective" approach; **(2)** the limitation of techniques that are "*reasonably likely to be used*" by **"*that*" entity** (again, a subjective assessment of a "*likeliness*" factor for each entity); **(3)** and an additional element that "**downstream**" identifiability is irrelevant. While (1) seems to be an expansive interpretation of case law (see below), elements (2) and (3) seem to be clearly contrary to current CJEU case law. Problems: – **Likely conflict with Article 8 of the Charter:** The definition of "personal data" in Article 8 of the Charter of Fundamental Rights (hereinafter the "Charter") is understood to be the definition in Directive 95/46 (see explanatory note of the Convention on the Charter). While the GDPR can be broader, if the GDPR becomes narrower than that definition, a conflict with the Charter would arise. In other words: the European legislator has no powers to change the definition of "*personal data*" below the understanding of Directive 95/46. ○ Directive 95/46 has (in the non-binding recital) highlighted that the "*means likely reasonable be used either by the controller or by any other person*" are relevant to determine identification. This wording describes the necessity of an objective assessment, or at least a requirement to take into account which other person will process that personal data. ○ The wording of Article 2(a) of the Directive clearly states that "*identification numbers*" (which usually constitute

For context: The definition referred to in Article 8 of the Charter is that in Directive 95/46. We hence copied the relevant texts from the old Directive in here: **Article 2(a) of Directive 95/46:** (a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; **Recital 26 of Directive 95/46:** (26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;	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.	"*pseudonyms*") were covered by Directive 95/46 and hence Article 8 of the Charter. ○ It is therefore clear that any definition that would exclude "*pseudonyms*" in many cases (or is prone to be understood that way by controllers, SAs and Courts) could get the GDPR into conflict with the Charter and hence create more legal instability compared to the current (well-established) understanding. – **CJEU Case Law does not back this change:** There are numerous cases by the CJEU on the definition of "*personal data*", but this proposed change seems to solely rely on an extensive and selective interpretation of C-413/23P EDPS v SRB. A ruling with a very specific fact pattern – which still seems to conflict with the proposed version: ○ The case in SRB was (see § 24 of the ruling) a situation where 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. ○ In the case CJEU also highlights 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 highlights multiple times in the ruling that this case was about the EDPS being correct that a "*pseudonym*" was "*in any case*" personal data (see §§ 68, 73, 80, 82 and 86). This does not allow to assume the opposite in any case.

		○ The CJEU highlighted the "*broad interpretation*" (§ 54) and the need for a case-by-case analysis (§100), making the ruling a questionable basis to justify changes to a general law. In a broader context the following rulings would have to also be taken into account, which were not taken into account when allegedly "*clarifying*" Article 4(1) GDPR, which only allows the conclusion that the aim is clearly to lower the standard of protection (mostly also cited in EDPS v SRB): ○ C-582/14 *Breyer* – A 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-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 country to the proposed draft. ○ 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). ○ C-683/21 – 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* – ff

		○ 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*.") – **Confusion rather than simplification:** It is unclear how e.g. an "identifier" in the existing definition or the option to be able to "*single out*" a person in the current GDPR recital would interact with the added provision and – especially – the added new recital 25 (see below). Multiple sources would be necessary to clarify what personal data actually means: ○ Dir 95/46 and Art 8 CFR (forming "*treaty law*") ○ Recital 26 GDPR (e.g. "*singling out*") ○ Recital 25 of the Omnibus and ○ the amended GDPR paragraph ○ versus the current GDPR paragraph; – **Complex assessment:** In practice an increasingly subjective assessment with many elements is very difficult to enforce. Anything is arguable if "*that*" (specific) controller would "*likely*" use a specific technique to identify a person: ○ Would a Bank use this? *Never*. ○ Google? *Maybe*. ○ An SME? *Probably not technically able.* ○ A hacker? *For sure.* It would require complex case-by-case assessments. – **Chicken and Egg Issue:** Given that also Article 15 GDPR would then not apply, a massive legal "chicken and egg" issue may arise, where data subjects (lacking any information about the processing) cannot prove anymore that their rights are even engaged. Thus effectively depriving them of said rights.

		– **SA enforcement massively complicated:** SAs may also find it harder to determine whether they have jurisdiction in a case. In reality SAs have little capacity or technical know-how to make such assessments for controller. Massive enforcement gaps are likely created by such (complex) subjective multi-factor tests, to even just know if the GDPR applies. – **Risk of compliance avoidance:** Companies could deliberately separate elements that need a *name* or *email* (e.g. billing via Apple Pay) from the service (e.g. an app) that only needs a *user number* or alike to "escape" the GDPR. Even though from a data subject side, just a tiny part of the processing is "split" and the user experience (e.g. "lock out from apps", tracking, sale of data) is exactly the same, the GDPR would then not apply anymore. Real Life Examples: – **Computers use exclusively "Pseudonyms":** Modern computer system identifiy people not by name; like "John Smith"; but under a random number, called "Universally Unique ID" (UUIDs). In an additional table, human-readable data like name or email are linked to that UUID. However, many non-user facing services (e.g. online tracking) may not have such a "linking table" or could easily "outsource" such a table. Therefore (since 1995) there mere existence of an identifier is covered by the GDPR and Article 8 of the Charter. The wording introduced could challenge this understanding. – **Tracking IDs:** Online Advertising IDs are largely random IDs to "single out" a person. However, the person may not be "identified" as "John Smith"; o Even though all players only use "IDs" it is easily possible to attribute that to people. See last week's reporting about the possibility to track EU Officials via such (ID based) online advertisement networks to their home, when previously present at the Berlaymont Building. o Under the proposed definition, the "*likeliness*" that any specific controller in the online advertisement space would

		engage in such an action becomes the determinant as to whether that particular controller's activities are exempt from the GDPR or not. – **Outsourcing:** Digital Services outsource payment and associated management of billing data (e.g. Stripe, Google Pay, Apple Pay) and therefore have limited "direct" contact with users in a way that requires identification as in "name and date of birth". Nevertheless, such apps or services clearly have identified users – but likely only under a number or other ID. – **"Login with Facebook/Google…":** User management is increasingly outsourced to third parties. Depending on the definition and configuration a controller only gets a UUID back and never knows the (real) name or email of the user. However, such a person can still be "identified" and/or is "identifiable" via an ID. – **Gay Dating App Example:** The gay dating app "Grindr" is mainly used for casual hookups. o Nevertheless, Grindr installed an SDK by Twitter in the app (a second "entity" according to the new definition). o That SDK forward IDs for online Advertisement to more than 4000 recipients. All of these advertisement partners only got an ID and the fact that that user is Gindr. I forwarded the fact the a person with a specific Google Advertising ID uses "Grindr" at a specific geolocation to thousands of advertisement partners. For these partners, the person is only known under the ID, not with name or birth date.
(15) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;	(15) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which **directly** reveal **information specifically** about his or her health status;	See changes on **Article 9(1) GDPR** below.

	(32) terminal equipment' means terminal equipment as set out in Article 1(1) of Directive 2008/63/EC; **(33) for 'electronic communications networks' and 'electronic communications services' the definitions of Article 2(1) and (4) of Directive (EU) 2018/1972 shall apply;** **(34) 'electronic communication service' means a service as defined in Article 2(4) of Directive 2018/1972;** **(35) 'web browser' means web browser as defined in Article 2(11) of Regulation (EU) 2022/1925;** **(36) 'operating system' means an operating system as defined in Article 2(10) of Regulation (EU) 2022/1925;** **(37) 'mobile application' means a mobile application as defined in Article 3(2) of Directive (EU) 2016/2102;** **(38) 'media service' means a media service as defined in Article 2(1) of Regulation (EU) 2024/1083;'(39) '(5) media service provider' means a media service provider as defined in Article 2(2) of Regulation (EU) 2024/1083;**	These definitions are necessary because Article 5(3) of the ePrivacy Directive is moved to the GDPR (see below).

Article 9 - Processing of special categories of personal data		
Current version	**Proposed version**	**Comments**
1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	1. Processing of personal data ~~revealing~~ **that directly reveals in relation to a specific data subject** racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, **his or her health status (data concerning health) or sex life or sexual orientation** and the processing of genetic data or of biometric data for the purpose of uniquely identifying a natural person ~~data concerning health or data concerning a natural person's sex life or sexual orientation~~ shall be prohibited. **Connected Recitals:** (26) In order to ensure a high level of protection of the fundamental rights and freedoms of natural persons, the notion of personal data is to be interpreted broadly. Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Special categories of personal data are therefore afforded enhanced protection under Regulation (EU) 2016/679. In line of the principle of proportionality enshrined in the Charter, such enhanced protection is justified only when the processing could create significant risks to the fundamental rights and freedoms of natural	The definition of special categories data in the proposed version is narrowed down compared to the current version. This narrowing down also contrasts the CJEU rulings C-101/01 Lindqvist, C-184/20 Vyriausioji tarnybinės etikos komisija or C-21/23 *Lindenapotheke*. It is hence not any "clarification" but a "rewriting" of the GDPR. Controllers often report that it is hard to separate sensitive data from other data, which is understandable, but on the other hand typically especially data subjects that "hide" or "protect" such information (and it can hence only be "*deduced*") are especially in need of protection. Problems: – **Violation of Convention 108:** The current wording "*revealing*" is taken from Article 6 of the Council of Europe Convention 108, signed by all EU Member States. Changing this definition would violate duties under the Convention. The Commission draft seems to not having taken the EU's duties under Convention 108 into account (at least it is not cited in the document, there was no impact assessment that may have brought this into scope). – **Direct Copy/Paste and Overturning of CJEU:** It is clear, that this change is not about "clarification" but about overturning the relevant CJEU rulings: ○ The change is intended to only covers information if there is "*significant risk*". If the data does not concerns "*a specific person*" "*with certainty*" and if any "*intellectual operation involving comparison, cross-referencing, collation or deduction*" if necessary to infer the existence of special

	persons, bearing in mind that Regulation (EU) 2019/679 applies to the processing of all information that constitutes personal data as defined in Regulation (EU) 2016/679. However, for most of the types of personal data listed in Article 9(1) of that Regulation, there are no such significant risks where the personal data are not inherently sensitive but are only indirectly liable of revealing sensitive information, for example where an individual's sexual orientation or health status can be inferred only by means of an intellectual operation involving comparison, cross-referencing, collation or deduction. No significant risks exist either in situations where the sensitive information would not concern with certainty a specific natural person. In such situations the general protection of Articles 5 and 6 of Regulation (EU) 2016/679 suffices, without the need to have in place a prohibition of processing under Article 9 of that Regulation. Therefore, the scope of application of Article 9 should be adjusted accordingly. The enhanced protection should be granted only to personal data which directly reveals in relation to a specific data subject racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health status (data concerning health), sex life or sexual orientation. The enhanced protection of genetic data and biometric data should remain untouched because of their unique and specific characteristics.	category data, the data would not be covered by Article 9 GDPR (see recital 26). ○ The wording of the proposed Recital 26 is a direct and flipped copy of the wording of the CJEU in § 123 of ruling in C-184/20 *OT*: "*the verb 'reveal' is consistent with the taking into account of processing not only of inherently sensitive data, but also of data revealing information of that nature indirectly, following an intellectual operation involving deduction or cross-referencing*". ○ The COM has therefore taken the exact wording of the controlling CJEU ruling and clearly tries to legislate against that CJEU case law to overturn it. ○ Further CJEU rulings to the same result can be found in C-252/21 *Bundeskartellamt*, §§ 69 and 70 or C-446/21 *Schrems* § 73. – **Narrowness:** The text of the Article 9(1) as proposed "*directly reveals*" could be understood to mean that only "*I am gay*" or "*I have cancer*" would qualify anymore, however for decades "inference" of information is standard practice (e.g. teenage pregnancy based on grocery shopping, sexual orientation or drug use from unrealted "like" data or exploitation of political leanings calculated from Facebook data by "Cambridge Analytica"). The wording "*directly reveals*" makes such inferences of special categories of data not be covered by Art 9. Especially as "big data" or AI systems only calculate a correlation between certain data, without necessarily putting people on a list of "pregnant" or "gay" people. In such cases no data that is "*directly*" linking to a sensitive category (there is no "table" of pregnant or gay people), but the impact is nevertheless directly felt, because the "grouping" happens via correlations (à la "other people like you, also bought diapers"). – **Deduction excluded from the definition:** If such information can be deduced, such as when an employer uses statistics on bathroom breaks to "*deduce*" that an employee is sick, that person would not be covered by Article 9 GDPR.

		– **Information shared versus withheld:** From a data subject perspective the illogical situation would appear that once a person published or shares sensitive data (e.g. "directly reveals" that the person has cancer) it would get protection under Article 9, while if it withholds such information (to protect itself) it would not enjoy the protection under Article 9 GDPR if such data is "deduced". Real Life Examples: – In practice ***noyb* has hardly seen a case where sensitive data is "directly revealed"**. Data subjects usually raise concerns over data that can be "found out" about them via modern technological means. This means that Art 9 would (in practice) largely lose its application. – **Most online advertisement** is just "deduced" information (e.g. a likeliness that a person is leaning liberal/conservative), also relying on correlations ("*people who relate to an item with an ID of 2378333 also like things with ID 2838383*") which can code for a political leaning, sexual practice or a certain health condition. – *noyb* had a case where a **woman lost her child during pregnancy,** but continuously got advertisement for kids items – progressing with the (theoretical) age of the kid. The woman never put her pregnancy status online, but online advertisement systems "deduced" the pregnancy and further "deduced" that the could should now be of a certain age – re-traumatizing the woman over and over. Under the proposal she would typically lose her Article 9 rights. – Grindr argued that using a **"Gay dating app"** would not fall under Article 9 GDPR, because women or straight people could also download it, as argued in Norway. Just recently the Norwegian courts have (after 5 years (!) of litigation over the application of Article 9) rejected this argument by Grindr. – The Austrian Postal Service used geolocation data and other information to "*deduce*" that a **person may vote for a specific party**, to then sell the addresses for postal advertisement of the relevant party, it was ultimately penalized with € 16 million.

		– In the case leading up to C-446/21 *Schrems*, Meta argued that only explicitly filled in political views in the profile of a Facebook user qualifies as Article 9 data, while just "*deduced*" information on political leanings (e.g. for online advertisement and political manipulation) would not fall under Article 9, but Article 6. This was rejected by the courts.
	(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. **(l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the verification is under the sole control of the data subject.** **5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid, to the greatest possible extent, 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**	***Note:* For many other problems with the "AI" allowances in the draft, see below at the draft *Article 88c*.** **On (2)(k) and (5):** Sub-paragraph (k) adds a provision allowing to use even the (under the draft narrowly defined) sensitive data for AI training - but also "*operation*" of an AI system. It also refers to the AI Act for a definition of AI – which is extremely broad. **On (2)(l):** Sub-paragraph (l) concerns the use of local face recognition and alike. We have not further analysed this provision. Problems in relation to (2)(k) and (5): – **Lack of a Proportionally Assessment.** Any limitation of the rights under Article 8 of the Charter needs to be proportionate under Art 52 of the Charter. 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: o It does not seem that the Commission has ensured to have the necessary evidence to show the need of 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). o Contrary to the legal duties of the legislator under Art 8 and 52 of the Charter, Recital 29 seems to be only concerned with the law being disproportionate for the entity interfering with the right to data protection. It is unheard of that the lack of a proportionality assessment is not just publicly documents, but

	undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties. **Connected Recitals:** (29) 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.	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. ○ Elements in Recital 29 like that data may be processed that is "*not necessary*" indicates 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 Art 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. – **Broad scope of application:** The GDPR would refer to the extremely broad definition of the AI Act. This broad definition was meant to have broad protections. Many "traditional" processing activities would fall under that definition. Using this broad definition for an exemption would lead to an extremely broad privilege in the GDPR. It is very likely that this would go far beyond a "proportionate" limitation of Art 8 in light of the Charter. – **Training and *Operation* of AI?** While there is a debate that the training of personal data could be a legitimate interest, it would hardly be compatible with Art 8(1) and (2) of the Charter and would never "survive" a proportionality test under Art 52(1) of the Charter if the mere **"*operation*" of a specific *technology*** is by default legal, especially for sensitive data. ○ 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*". This can itself create more legal uncertainty. ○ It seems hard to explain why the European legislator has come to the conclusion that only one processing technology (AI) that is especially risky would meet the criteria of Article 52 of

	(30) Biometric data, as defined in Article 4(14) of Regulation (EU) 2016/679, means processing of certain characteristics of a natural person through a specific technical means and which allows or confirms the unique identification of that person. The notion of biometric data includes two distinct functions, namely the identification of a natural person or the verification (also called authentication) of his or her claimed identity, both of which rely on different technical processes. The identification process is based on a 'one-to-many' search of the data subject's biometric data in a database, while the verification process is based on a 'one-to-one' comparison of biometric data provided by the data subject, who is thereby claiming his or her identity. Derogating from the prohibition to process biometric data under Article 9(1) of the Regulation should also be allowed where the verification of the claimed identity of the data subject is necessary for a purpose pursued by the controller, and suitable safeguards apply to enable the data subject to have sole control of the verification process. For example, where the biometric data are stored solely at the side of the data subject or are stored at the side of the controller in an encrypted form and the encryption key or equivalent means is held solely by the data subject, that processing is not likely to create significant risks to his or her fundamental rights and freedoms. The controller does not gain knowledge of the biometric data or only for a very limited time during the verification process.	the Charter, while any other form of processing (e.g a traditional database or algorithm) would not be allowed under Article 9(2) GDPR. – **Minimisation "Light"?** Paragraph 5 adds "limitations" to the use of sensitive data for AI training, which consists of a highly conditional ("*appropriate*", "*to the greatest extent possible*") duty to "*avoid*" such collection or remove such information if does not require "*disproportionate effort*". 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. – **No Balancing Test:** 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 absolute 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 and more legal uncertainty. The different regimes could be especially problematic if a controller cannot distinguish between "sensitive" and "normal" personal data. – **Broad AI privilege:** The "privilege" on AI goes beyond just training, 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". – **Weakened protection:** It seems the protections under Article 9 seem weaker than for Article 6 data.

Article 12 - Transparent information, communication and modalities for the exercise of the rights of the data subject		
(3) 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.	(3) 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 because he or she exploits 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**. **Connected Recitals**: (31) 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 rights under Regulation (EU) 2016/679. By contrast, it should be clarified in Article 12	**This change seems to be inspired by a Lobby 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. We are not aware of a larger debate in other EU Member States.** **All data subjects' rights are affected:** While the change seems to be intended only to cover access requests under Article 15 (see recital), the amendment to the text is *in fact* applicable to all data subjects' rights (i.e. Article 15-22; not to Article 13 and 14 since they are not connected to a request by the data subject). **Access right used for civil procedures:** The issue seems to stem from data subjects using the right to access to generate evidence for civil procedures. This is logical, as more and more data (e.g. in the employment context) are only available to the controller (e.g. because access is technically cut). This is especially debated in Germany – but does usually not feature as a "*problem*" in other Member States. There seems to be no objective evidence that would prove this is a broader issue. 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. Problems: – **Conflict with Article 8 of the Charter:** The right to access under Article 15 GDPR is ***itself* a *freestanding* fundamental right** under Article 8 of the Charter, as is the right to rectification "and the right to have it rectified": "*Everyone has the right of access to data which has been collected concerning him or her*".

	of the Regulation that the right of access, which is from the outset favourable to data subjects, should not be abused or exploited by 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.	○ It is not an "*annex right*". Therefore, the exercise of the right of access may be used for any purpose, just like the "*right to free speech*" or "*the right to property*". ○ See also C-307/22 *FT*, §§ 29 to 52, C-579/21 *Pankki S*, § 88 and GA opinion in C-526/24 *Brillen Rottler*) where the CJEU made clear that there is no "purpose" or "motive" limitation on the Right to Access under Art 15 (and hence under Article 8(2) of the Charter). – **Conflict with Article 52 of the Charter:** Adding a condition to the exercise of the right provided by Article 8 amounts to restrictaion of the full application of the article. Limiting the grounds for which an access request can be made so extensively is stricter than necessary. Likely, this is not lawful in accordance with Article 52 of the Charter: "*Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*." – **Informational self-determination:** 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" but the core right. – **Clearly unintended scope:** If the Recital is compared to the text, it seems clear that the drafters did not properly read Article 12: The intent seems to be only narrowing the rights under Article 15 GDPR, but the scope of Article 12(3) is Article 13 to 22 and 34. This would lead to entirely absurd or circular consequences: ○ If the right to rectification cannot be used for "*purposes other than data protection*", would a person still be able to correct false financial information for the purpose of getting a better credit score and hence pay less – a "*financial purpose*"?

		○ Can a data subject request deletion (e.g. "right to delisting" under C-131/12 *Google Spain*) for economic, job or reputational reasons? – **Clear attempt to overthrow CJEU case-law:** The change is an attempt to overthrow what the CJEU held in the past See also C-307/22 *FT*, §§ 29 to 52, C-579/21 *Pankki S*, § 88 and GA opinion in C-526/24 *Brillen Rottler*). In § 88 of Pankki S the CJEU summarized the law as follows: "*the context in which that data subject requests access to the information referred to in Article 15(1) of the GDPR cannot have any influence on the scope of that right*." – **No gap to fill:** 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. There is simply no gap in legal protection this provision could close. – **"Purpose Limitation" for User 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. E.g. 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 should not be considered abusive solely because the motivation for the request is not only in the protection of the data of the person making the request. The same is true in case an access request is made in course of academic research in accordance with Article 13 of the Charter. – **Burden of proof reduced:** The amendment plans to reduce 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 - which is a rather subjective test.

		○ 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. ○ Any likely motivation other than data protection could justify the controller's rejection of a request. E.g. the data subject is an employee, journalist, opponent in any kind of litigation. ○ The proposed text seems to condemn 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 intendt/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. A requirement that was already rejected by the CJEU. ○ Overall, it could *de facto* lead to a reversal of the burden of proof, as data subjects would have to bring a case (lasting years oftentimes) to overcome the argument of being "excessive" and have to show their interests in the course of such a case. Real-Life Problems: – Requests by journalists, employees, consumers in a pending dispute, people in pending litigation and many more would lose their rights under Article 8(2) of the Charter and Article 15 GDRP. – In reality the enforcement of the Right to Access is almost impossible for an average data subject for one of two reasons: ○ Costs often amount to thousands of Euros via the Civil Courts (Article 79 GDPR), many jurisdictions take years to decide,

		and Courts have no investigative powers to find out what data is actually processed ("*he said/she said*" trials); ○ Or, if enforcement action is taken via the SA route, it is either not processed by SAs (see Article 77 GDPR, where we note the Commission's inaccurate view that there is no "right" to a decision under Article 77 GDPR in the "GDPR Procedure Regulation" negotiations), or SA procedures take years (see below) and SAs never use relevant investigative powers from our experience. This means that **additional exemptions based on "*beliefs*" of controllers would make Article 15 GDPR meaningless** in practice – especially forrecalcitrant controllers. – The daily experience of *noyb* is that the vast majority of requests are either partially or not at all responded to. We internally estimate that at best 10% of requests are granted fully and in time. Statistically the problem with Art 15 is not mainly "abusive" request, but "abusive non-compliance", we therefore doubt that the Commission has relevant evidence that substantiate these changes. – Law needs to regulate "conflicts". 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 legislator must take these players also into account. For example: ○ 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. ○ The amendment will likely further delay the exercise of Article 15 rights. Already under the current text, massive delays apply: it can regularly take 5+ years to get access via a complaint by a SA, if a controller engages in delay tactics. ○ Especially "problematic" controllers regularly ask data subjects for their motivation to make a request (in particular access requests) and already argue that these reasons are "abusive". This triggers year-long procedures before Courts

		and SAs. Art 15 is already by far the most common reason for complaints. More reasons for rejections will likely lead to even more complaints. ○ "Problematic" controllers further engage in countless "questions" that are regularly based on bad processes or obvious delay tactics (e.g. asking an irrelevant "question" exactly one month after the request, pretending that this would reset the deadline under Art 12(3) GDPR again). – Specific problems arise from the "information imbalance" that Art 15 GDPR tries to overcome: ○ 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 than to ask for "all data" to avoid controllers "hiding" problematic data by not disclosing where such data could be. ○ Especially in consumer or employment contexts, most evidence is not in "paper form" anymore (e.g. time sheets or communication), but digital (e.g. online systems, chat bots). 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. ○ It is not a "bug" but a core principle of "informational self-determination" that data subjects have full access to their own data, for whatever purpose they like to pursue. – For example: 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;

Article 13 - Information to be provided where personal data are collected from the data subject		
4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.	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.** **Connected Recitals**: (32) 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	This proposed amendment uses vague wording, enabling misuse and creatinges legal uncertainty. Problems: – **Charter implications:** 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 it would be unable to know if it has rights under Art 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. – **Confusing wording:** The wording is extremely unclear and unpredictable: o It is unclear, what a "*clear and circumscribed relationship*" between the data subject and the controller is or o what would constitute a "*not data-intensive*" „*activity*". According to the Recitals, this is supposed to cover the relationship between a craftsman and their clients. However, the wording of the provision could also be interpreted more broadly. 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. This should only be the case then the controller also provided the information to the data subject e.g. when concluding a contract. Definitions that would be clearer: o Limitation to "face to face" interactions in a B2C situation, for example using the definition of "*off-premises contract*" in Article 2(8) of Directive 2011/83/EU.

	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 expect that the data subject already has the information referred to in paragraphs 1, 2 or 3 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. In such a context, 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	○ Clear definition of the size of the company that can use such an exemption. – **Less onerous way?** The provision could easily be made more likely to be acceptable by e.g. requiring that such information must be given upon request and/or also orally. This would still allow a data subject to at least ask an SME in an email or in person and understand matters when in doubt. It seems questionable if the access to such information is fully blocked by law. – **Likely shift of the information upon access requests:** the only way for the data subject to receive the other information mentioned in Article 13 would be to make an access request to the controller under Article 15. This might leave the controllers with even more work than having a nuanced (e.g. on request) solution. – **Some information not covered, Art 8 of the Charter issues:** Some information (e.g. the legal basis for processing) is only available under Article 13 and not under Article 15, because the legislator assumed that Article 15 does not require it – because people got that information already. However, this would mean that such information would never be provided to the data subject - making 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. – **Information as to the exemption:** the controller should inform data subjects about the fact that it invoked this exemption and provide them with a link to the privacy policy; – **Informed consent:** This 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;

	15 of Regulation (EU) 2016/679that 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.	– **In reality hardly applicable for SMEs:** The exception will in practice 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.
Article 22 - Automated individual decision-making, including profiling		
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	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 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**	Paragraph 1 and 2 of Article 22 were combined in one paragraph. Paragraph 1 seems to be materially unchanged even if formulated differently (not as a right but as cases in which ADM is permissible). The (only) material change is connected to the exemption of the 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. Generally, Article 22 GDPR is not a requirement under the Charter, but Automated decision-making is mentioned in Art 9(1)(a) of Convection 108. Technical issue: – The references in Art 22(3) and (4) would also need to be amended to reflect that Art 22(2) would not exist anymore.

safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent.	**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. **Connected Recitals:** (33) 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.	Problems: – **Necessity requirement:** While generally "*necessary*" is not understood to mean that digital processing could be replaced by "*pen and paper*", a narrower view with regards to Art 22 seems to have been argued: ○ According to Art 22(2)(a) GDPR, "*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*." Art 29 guidelines p 23. ○ Therefore, if a less intrusive method than ADM is available and possible, ADM is not permissible for the performance of a contract (see e.g. Scholz, in Simitis, Hornung, Spiecker gen. Döhmann, Datenschutzrecht, Article 35 GDPR, margin numbers 44 (NOMOS 2025, 2nd Edition).) ○ This is supposed to be changed and for the assessment of the necessity it should not matter whether the decision could be taken otherwise than by solely automated means; – **Full discretion for the controller:** The controller therefore seems to have full discretion in whether to use ADM for the performance of, or entering into, a contract. This is quite a paradigm shift and will lead to more usage of ADM subjecting data subjects to automated decisions without (prior) human involvement. – **Covered by 6(1)(b) already:** It is questionable whether the requirement of necessity in Art 22(2)(a) GDPR adds anything (and if so, what) to the already existing requirement in Art 6(1)(b) GDPR. Since any decision made under Art 22 also needs a legal basis in Art 6(1) GDPR (see CJEU *Schufa* C-634/21 §67 et seqq); – **Risk of increasing the use of ADM:** Fully automated rejections to enter into a contract could become much more common. Fully

		automated selection processes for jobs, schools, universities etc. could become even more prevalent. – **Significant impact:** Being permanently subject to ADM will certainly have a significant impact on individuals' rights and freedoms, considering how common it is that algorithms still show an immense level of bias and often are unexplainable and thereforeproduce unfair, unreliable and incomprehensible results. Real-Life Examples: – In the feedback from data subjects, automated decisions (e.g. account suspensions) are increasingly regular and seen as **enormously frustrating**. o Many controllers that use ADM have an overall strategy to ideally "not interact" with consumers. o Protections under Article 22(3) GDPR (especially "human intervention") is regularly unavailable or meaningless (automated email response, signed with a generic name). Evidence for Changes: – While the current Art 22 GDPR is not well-drafted and confusing, the real-life problem does in our experience not lie in the "*necessary*" element, but in Art 22(3) and major compliance issues. – We therefore think that a reform to Art 22 GDPR may be warranted, but may need a more elaborate debate. We note that Article 22 GDPR was not in the scope of the Call for Evidence and additional input would be useful.

Article 33 - Notification of a personal data breach to the supervisory authority		
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. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. **In comparison wording of Article 34 GDPR:** (1) When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.	1. 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. **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. The proposal shall be submitted to the Commission within [months] of the entry into**	This amendment to Article 33 GDPR would raise the threshold for the obligation to notify a SA about a data breach "*unless* [its] *unlikely to result in a risk …*" to "*likely to result in a high risk*". The change is therefore two-fold: – The threshold is moved from "*a risk*" to "*high risk*" – The exemption ("unlikely") is turned into a condition for the duty to even kick in ("likely") While the high number of Data Breach Notifications (e.g. wrongly sent emails) has led to SAs generally just "*ignoring*" them, the change seems to be quite massive. Problems: – **"High Risk":** The threshold of a "hight risk" is still unclear, which becomes even more urgent to solve, given that SAs would now not be able to do a second assessment under Article 34(4) GDPR. – **Level Raised to Article 34 GDPR:** The wording of Article 33 would then be 1:1 the same as Art 34 GDPR. It is well-known that the number of notifications under Article 33 was a multitude compared to notifications under Article 34. If the current number of Art 34 notifications is taken as a realistic benchmark for future data breach notifications to SAs, we would see only the most extreme breaches reported. – **Overlap with Article 34(4) GDPR:** The proposed standard is basically the same standard as the notification of the data subjects themselves. This would regularly make Article 34(4) GDPR void since the cases only the SA has to be notified but not the data subjects would be limited to the cases Article 34(3) GDPR apply.

	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 referred to in paragraph 6 shall be reviewed 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.** **Connected Recitals:** (34) 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	– **No "face saving" way to reach an SA anymore?** Controllers are typically reluctant to notify data subjects due to the immense potential consequences of such a notification (damages claims, reputational harm). In turn this increased the likelihood of further damages. Having the same threshold might make it hard to "only" inform the SA, because it would typically trigger Art 34 too – which is not a positive development, because SAs would not be able to insist on further steps or help manage an incident. To ensure that (relevant) cases still reach SAs (even when a controller may decide to deliberately not inform the data subjects) the reporting threshold under Article 33 should not run in parallel, but continue to be somehow lower than in under Article 34 GDPR.

	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. 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 should be reviewed at least every three years and updated where necessary.	
Article 35 - Data protection impact assessment		
'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	**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**	The proposal allows for white/blacklists if a DPIA is necessary. This should replace national rules that were inconsistent or non-existent. We would welcome such a change. Given that this is merely a change in responsibilities, but no material change, we did not conduct further research into this proposal.

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.	**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.** **Connected Recital:** (35) 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.	

Article 41a		
	[Placeholder for mechanism to accompany the state of the art advancements for pseudonymisation technologies.]	In the document, the Commission seems to have foreseen a "placeholder" that would allow the Commission for further define what is "personal data" under Article 4(1) GDPR and allow the Commission to exclude certain processing from the GDPR. The idea was allegedly to use Implementing acts or delegated acts here. Problem: – **The Commission would be able to shape a right under the Charter:** This would allow the Commission to limit a fundamental right via Article 4(1) and a delegated act, which in turn could erode protections under Article 8 of the Charter; – It is very questionable if this would comply with EU Treaty Law.
Article 57 - Tasks		
1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: (k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);	1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: (k) ~~establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35~~(4); [Under discussion] **(w) set up regulatory sandboxes, i.e. the controlled framework set up by the supervisory authority which offers data controllers and/or processors and/or prospective data controllers and/or processors the possibility to test the compliance of specific techniques or technological solutions to be used for the data**	The idea of "regulatory sandboxes" is added to the tasks of the supervisory authorities. Problem: – **Lack of definition:** It is unclear what these "sandboxes" would entail and to what extent they would interfere with data subjects' rights. – **Independence and Conflict with Article 8(3) CFR:** To the extent that this would be a "discussion format", there may be an impact on SA independence under Article 8(3) of the Charter. o In Article 57(1)(d) GDPR the legislator has deliberately chosen toonly have general "promotion" of awareness for

	processing activities with the obligations under this Regulation or whether the data processing results in data that would be exempt from this Regulation ('anonymisation techniques').	controllers, but no 1:1 advice or cooperation, because the same SA would have to decide about complaints under Article 77 GDPR and would then be conflicted. We are aware that many SAs still engage in 1:1 advice, counselling or even cooperation with controllers, but this is strictly speaking *ultra vires* activity by SAs. ○ One-sided formats (only with one or more controllers) are in daily practice a path to pressure SAs into certain legal views, without having appropriate "*counter speech*" and an advocate for data subjects' rights. Practice has e.g. shown that the role of SAs in Codes of Conduct are often extremely frustrating for SAs (and controllers) because industry demands *must* be pushed back by SAs, when controllers understand them to be "negotiations" about the meaning of the law. – **SA capacity:** SAs generally highlight a lack of capacity. It is unclear how SAs would be able to dedicate sufficient resources to this additional task. Real Life Examples: – SAs regularly "cooperate" with, or "negotiate" or "informally approve" actions by controllers. Quickly thereafter they are then called to decide about this processing activity as an "independent" authority under Article 8(3) of the Charter. This leads to an inherent conflict of interest, because they would have to decide about their own previous legal advice. For example: ○ The Irish DPC approved that Meta may use Article 6(1)(b) GDPR for online advertisement in 10 confidential meetings. Months later *noyb* issued a complaint on this matter. The DPC then tried to influence the EDPB guidelines in the interest of Meta, delayed the procedure for years and ultimately lost

		before the EDPB. The CJEU confirmed that the view of the DPC was inaccurate and the processing was illegal in C-252/21 *Bundeskartellamt*. ○ The Hamburg SA has proposed to two newspapers ("Der Spiegel" and "Die Zeit") to introduce "Pay or Okay". Once the newspapers introduce the change, noyb got reports by users and filed a complaint under Art 77 GDPR, which the Hamburg SA, who now had to decide about its own legal advice with the newspapers. The SA stayed inactive over the complaint, so *noyb* sued the SA before the Courts. It will be questionable if the Hamburg SA could even "independently" decide these cases anymore – but there is also no option to switch the LSA in such a case to an SA that was not previously involved in giving controllers advice.
Article 64 - Opinion of the Board		
1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it: (a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);	1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it: ~~(a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);~~	Removal of duty, given that this duties around Article 35 was moved to the EDPB / Commission.

Article 70 - Tasks of the Board		
1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:	1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular: **(ha) 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 and for which no data protection impact assessment is required, pursuant to Article 35.** **(hb) prepare and transmit to the Commission a proposal for a common template and a common methodology for conducting data protection impact assessments, pursuant to Article 35.** **(hc) prepare and transmit to the Commission a proposal for a common template and a common methodology for conducting data protection impact assessments, pursuant to Article 35.**	New duty, given that duties around Article 35 was moved to the EDPB / Commission.

Article 88a - Processing of personal data in the context of terminal equipment		
	[Agreement between CNECT and JUST reached on the principles; text still subject to fine-tuning between the DGs:] **1. The processing of personal data on or from terminal equipment of a data subject shall be permitted if it is necessary solely for one of the following purposes:** **a) carrying out the transmission of an electronic communication over an electronic communications network; or** **b) providing a service explicitly requested by the data subject; or** **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; or** **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 this service.**	**Part 1: Terminal Equipment** ***Note:*** *The processing of non-personal data is still regulated in Article 5(3) ePrivacy (**see below**) under the current legal basis.* It seems that Article 88a now regulates the processing of personal data in a "terminal equipment" on 10 legal bases. Problems: - **Article 7 of the Charter.** Traditionally, the protection of a "termina equipment" is based on secrecy of communication under Art 7 of the Charter, not solely on Art 8. Hence, Art 5(3) of the ePrivacy was always covering legal persons and not just "personal data". The relationship between protections that the legislator has to provide under Art 7 and 8 of the Charter is unclear in the draft text or in the relevant recitals. The scope of Art. 5(3) ePrivacy Directive offers **protection for the device integrity**. This, read in conjunction with the proposed Article 88a of the GDPR, amounts to protection being lost with "just" applying the GDPR. This fundamentally weakens security of devices. - **Scope goes far beyond "Cookies":** While this provision is meant to replace the commonly known "cookie law", many other situations exist where data can be stored in a terminal equipment (e.g. personal data on a smart phone, PC or Smart TV). This is important to remember when analysing this draft.

	When the controller collects personal data solely for these purposes, it shall not be allowed to use this data for any other purpose, unless the processing is based on a Union or Member State law. **For any other purpose that those referred in the first subparagraph the processing shall comply with Article 6 and, where applicable, with Article 9.** **2. Where the processing is based on Article 6(1)(a), the following applies:** **(a) the data subject shall be able to [give consent or] refuse requests for consent in easy and intelligible manner with a single-click button or equivalent means;** **(b) the controller shall respect data subject's choice [to give consent] or refuse a request for consent for a period of at least [6 months], unless the processing is necessary only for shorter period of time. The controller shall not make a new request for consent for the same purpose within this period.**	- **Scope far beyond "access/storing":** The scope of Article 88a goes far beyond Article 5(3) GDPR: o Article 5(3) ePrivacy only regulated the "*storing of information, or the gaining of access to information already stored, in the terminal equipment*" – so in other words "crossing the line" into a device. o The new Article 88a would regulate **any "*processing*"** (!) of personal data **"*on or from*" a terminal equipment.** This would mean that: o even data that is processed in an app on a phone would fulfil the criteria ("*on*"), also o data that was originally entered on a phone or PC (e.g. booking a hotel room on a website) would be covered because it would be "*from*" a terminal device. - **Scope may be unintended:** It is very unclear if this broad scope was intended or is an error in the drafting process. Recital 37 repeats as examples ("*such as*") the current processing operations of Art 5(3) ("*storing*" and "*access*" or [new] "*collecting*"). There is no clear indication why the text of the Article was broadened. - **Relationship of 4 purposes and Article 6(1) or 9(2) unclear:** The text and the recital seem to be unclear to many readers, even persons within the EU institutions seem to have different understandings of the relationship of Art 88a(1) and Art 6(1) or 9(2). The following understandings have developed in the past days: o **Understanding A: Closed List.** Recital 37 speaks about the four new purposes being "*closed list of purposes solely for which the processing should be permitted*". This would mean that processing for other purposes would not be permitted (similar to the current Article 5(3) ePrivacy) and data "*on*" or "*from*" a terminal equipment would be limited to the four listed purposes

	3. Where processing is based on Article 6(1)(f) for the purpose of direct marketing, the data subject shall be able to exercise his or her right to object pursuant to Article 21(2) with a single-click button or equivalent means. **Connected Recitals:** (37) [Approach agreed, text still being fine-tuned] [The processing of personal data on or from the terminal equipment, such as by storing in that equipment information, accessing or otherwise collecting information from that terminal equipment that results into processing of personal data should be brought under one legal regime, which is the regime of Regulation (EU) 2016/679. The rules should apply independently from the legal relationship between a data subject and the terminal equipment which may be owned by another legal or natural person. In view of reducing the compliance burden and give legal clarity to controllers, and given that certain purposes of processing that pose a low risk to the rights and freedoms of data subjects or when such processing is necessary to provide a service requested by the data subject, this Regulation should define a closed list of purposes solely for which the processing should be permitted. For those purposes this Regulation provides therefore the legal basis of processing in compliance with Article 6 of Regulation (EU) 2016/679. The controller, such as a media service provider, may mandate a processor, such as market research company, to carry out the processing on its behalf. Processing for any other purpose of the data initially collected for one of the	in (a) to (d). This would however conflict with 88a(2) that again speaks about consent as a legal basis, which is not mentioned in paragraph 1 (a) to (d). ○ **Understanding B: Addition to Art 6(1) or 9(2):** The second reading is that paragraph 1 (a) to (d) is added to the legal basis in Article 6(1) and/or 9(2) GDPR. This would make a combined list of 10 (!) legal basis for "normal" personal data, even if some processing operations would overlap (e.g. "security" under (d) and Article 6(1)(f) GDPR). This would strangely have the result, that if data is "on" or "from" an (especially protected) terminal equipment, it would have more available legal basis than other data and hence be less protected. However, this would be the plain reading of the text "*For any other purpose that those referred in the first subparagraph the processing shall comply with Article 6 and, where applicable, with Article 9*". The law does not say something like "*for any other processing operation*" (e.g. other than access and storage), which would explain that there is processing before/after, but says that such data can be used for any other "purpose" under Art 6(1) and/or Art 9(2). ○ The EDPB already stated about the current legal framework that „*Art. 6 GDPR cannot be relied upon by controllers in order to lower the additional protection provided by art. 5(3) ePrivacy directive*." (Guidelines 01/2020, para. 15). This is exactly what this reading of the proposal would do. ○ **Understanding C: Combined List:** The final understanding is that (just like it is argued for Art 6(1) and 9(2) GDPR) this is a combined list, where (1) the purposes under 88a(1) must be met and a legal basis under Article 6(1) and/or 9(2) must be established. This would result in "combined" protections and is

	purposes listed should not be allowed unless Member States or Union law provides for it. For any other purpose than those defined in the closed list, the controller should be able to rely on one of the legal bases of processing pursuant to Article 6 of Regulation (EU) 2016/679 and, where processing of special categories of data is involved, the controller should comply with the requirements of Article 9 of Regulation (EU) 2016/679. It is the responsibility of the controller to choose the appropriate legal basis of the intended processing. (38) 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. This could similarly be the case when the data subject exercises his or her right to object to direct marketing, which according to Article 21(2) ofRegulation (EU) 2016/679 does not depend on grounds relating to data subject's particular situation. The controller should therefore be obliged to respect the data subject's choices to refuse a request for consent or object to the processing for direct marketing for at least a certain period.	probably the only understanding that would avoid many of the problems of the other understandings. The fact that experts cannot agree on what is intended by the draft is highly concerning regarding legal certainty, as well as the draft's quality. - **Legal basis in (a) to (d) go beyond Art 6(1) and would again be hard to argue under Art 7 and 8 of the Charter:** While the four purposes can be seen as generally agreeable, it must be noted that they are formulated as "**absolute allowances"**, which makes it likely that they again will violate the the GDPR and (partly) the Charter: o 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. o Also, "*maintaining the security of a service"* can be very broad and can allow massive "*searching*" of locally stored data (towards a "remote search" of devices). This could entail unintended consequences (see discussions about "upload filters" and alike). Article 88a could allow extremely invasive techniques on user devices (!) that go far beyond anything that would likely be accepted by the CJEU under Art 7 and 8 of the Charter (see "data retention" and other case law). - **Unclear interplay with other changes**: The provision seems to create strange results when combined with other changes in the draft: o This provision, when read together with the new proposal on the **definition of personal data** in Article 4(1) GDPR, creates less clarity. What happens if data is personal for one controller and not personal for the other one?

		▪ For example: If a media company allows 800 advertising partners to track people on its website, the media website can usually not even know/access the tracking IDs that are set by scripts loaded in iFrames and alike. So far, they may be joint controller (see C-40/17 *Fashion ID*). Who would fall under Art 88a with a new personal data definition? ▪ Would a media website then fall under the (more restrictive) Article 5(3) ePrivacy, because it does not have "personal data" available to it anymore? ▪ Many of these questions cannot be solved here, but could arise if multiple elements get changed in inconsistent ways. ○ Equally, the fact that **AI training and operation** is defined as a "legitimate interest" and access to the terminal equipment is (under one reading) allowed for a "legitimate interest" would mean that (if technically possible) and a subsequent "balancing" is seen as positive by the controller AI companies could "pull" personal data from devices like smartphones and PCs. <u>Expected practice:</u> – We will likely see a spike in data processing for "*security purposes*" and "*aggregated information*", and it will remain unclear what both of them mean in each individual case; – Users may be confused with the additional options that they are presented with on top of legitimate interest, consent; – Already now in common cookie banners, users are commonly mislead with deceptive design: This will just increase; – We could go back to a situation where, if consent is not refused, it is seen as granted (alternatively, this logic is achieved through relying on Article 6(1)(f) GDPR);

		– As there is no device protection foreseen in the new GDPR provision, controllers would likely access information on devices (in particular Google on Android, Apple on iOS, Microsoft on Windows) or install something on users' devices (i.e. when surfing the web, or by updating apps/software) and use the information obtained for their interests (on the basis of Article 6(1)(f) GDPR). This will be particularly true for AI purposes; – It was reported that Google may access information on Andoid devices for AI training. Given that Article 88c would declare such processing as a "legitimate interest" and Article 88a allows access to locally stored data for "legitimate interests"; – Accessing any personal data on a device like Microsoft Copilot Recall (see here) will likewise be covered and allowed; – Kernel-level software for security purposes that may have access to almost all data on a device may be lawfully used. See this article for an example for a video game company.

		Part 2: New Rules on Consent
		
		- **Consent fatigue:** The proposal requires a "One Click" option to reject consent requests. While this would overcome issues such as consent buttons being hidden in a "second layer", it would be insufficient to overcome most other "dark patterns" that most SAs have already prohibited (overview on out ruled dark patterns here). For example:
		  o Just having a tiny link somewhere in the text of the banner to reject (e.g. a "reject" in the explanatory text where no one finds it) and a contrasting huge button for consent, would still be "one click", but hardly manageable for users.
		  o The "one click" requirement would fall behind most SAs current guidelines. The more consistent approach would be a comparative rule like Article 7(3) "*It shall be as easy to withdraw as to give consent*." For example, "*It shall be as easy to **reject and** withdraw as to give consent*". Only these two words in Art 7(3) could solve the issue (largely in line with SA rules on colours, shapes, sizes and alike) and in broad way.
		- **Tech Neutrality:** The provision in paragraph 3 seems to apply to any consent under Article 6(1)(a) – no matter if in an online or offline context. Consent can be given orally, on paper or under Art 6(1)(a) also in an "implicit" way (e.g. group for a picture). Wording of a law that requires a "button" would – at least based on the text – also apply in such situations. This is another reason, why a "tech neutral" wording like "*as easy as*" should be favoured.

		- **Missing Link to Art 9(1)(a) or 22(1)(c):** Surprisingly no reference is made to other consent situations, such as Art 9(1)(a) or the new Art 22(1)(c), which also require consent. o It would be illogical to only have a "one click" requirement for "normal" data, but not for "sensitive" data or automated decisions. Again, the higher risk processing would then have less protection (as with other proposed changes). o We also want to note that other laws increasingly (e.g. DMA or ePrivacy) refer to "consent" in the GDPR and the "dark pattern" issue is therefore also relevant for many other laws. 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". - **Scope & Structure:** Definitions around requirements for consent are generally regulated in Article 7 GDPR. It is unclear why these rules are now in another Article and only linked to Article 6(1)(a). o **Time limit & Additional tracking:** The law suggests that consent requests may not be repeated within 6 months, which is useful. However, this may require to track users (or at least place a non-personal "no request" cookie that lapses after 6 months) to ensure that controllers actually know that they asked a data subject already. This may not be (technically) possible in all settings. - **No provision on dark patterns:** Websites like https://www.vogue.fr/ use many deceptive design patterns for obtaining consent**.** The provision misses the opportunity to regulate them;

		- **Unclear terms:** Design-wise it is not clear what "*single-click button or equivalent means*" exactly means. This will not be helpful in the discussion about deceptive design and these designs will continue to exist.
Article 88b - Automated and machine-readable indications of data subject's choices		
	[Agreement between CNECT and JUST reached on the principles; text still subject to fine-tuning between the DGs:] **1. The data subject shall be able to [give consent or] refuse a request for consent and exercise the right to object pursuant to Article 21(2) through automated and machine-readable means.** **2. Controllers shall ensure that their online interfaces are able to interpret the automated and machine-readable indications of data subjects' [acceptance or] refusal or acceptance to a request for consent and the exercise of the right to object as referred to in paragraph 1 and respect those indications. This obligation shall apply [6**	Generally, the existence of this provision is a good sign for having less consent requests. It could overcome the "cookie banner" that is problematic for controllers and data subjects. The EU would "catch up" to California and other US States that now use "Global Privacy Control". The relevant elements (website endpoints and software vendors) seem to be properly covered. Problems: – **Withdrawal:** The law regulates consent, objection and the (new) notion of a "refusal" of consent. The "withdrawal" is not regulated. Given that Art 7(3) GDPR requires that a "withdrawal" is "as easy" as giving consent, controllers may (in combination of Art 88b and

	months] following the publication of the harmonised standards pursuant to paragraph 4. **3. The obligation pursuant to paragraph 2 shall not apply to controllers that are media service providers when providing a media service.** **4. Controllers which meet the harmonised standards or parts thereof, the references of which are published in the Official Journal of the European Union, shall be presumed to be in conformity with the essential requirements laid down in paragraph 2 to the extent that those requirements are covered by such harmonised standards or parts thereof.** **5. After taking into account relevant international and European standards and self-regulatory initiatives, the Commission shall, in accordance with Article 10(1) of Regulation (EU) 1025/2012, request one or more European standardisation organisations to draft standards that satisfy the requirements laid down in paragraph 1 of this Article.**	Art 7(3) GDPR) be required to also accept withdrawals of consent via a signal. However, this could be clarified in law. – **No standards set:** The standard(s) are not set by an EU institution, which could lead to a year-long standardization process. The advertisement industry in particular may try and drag out the standardization process for as long as possible. It is also possible that multiple standards coexist creating a higher burden on controllers/OS providers. It is also unclear in which concrete circumstances the Commission would consider a delegated act; – **No red lines in law:** The law leaves the details of a standard wide open. They could be rather "rough cut" signals like DNT or GPC, or more nuanced approaches like ADPC. Most of the usefulness (and possible abuse) of such a system would be the matter of implementation, which would lie outside of democratic control in a standardization body (that are already under massive critique in other areas). – **Opt-out:** We could go back to a situation where if consent is not refused it is seen as granted (alternatively, this logic is achieved through relying on Article 6(1)(f) GDPR – see provisions in Article 88a GDPR); – **No changes for medias websites:** The definition of journalistic pages via "media service providers" (as used in Article 2(2) of Regulation (EU) 2024/1083) seems to ensure that there is sufficient legal certainty as to the meaning of the provision. Recital 39 explain that media sites are exempt from the law, to protect their economic interests. It is not clear if such a sectorial limitation can be justified under Art 8, 20 and 52 of the Charter.

	6. The Commission shall be empowered to set out in a delegated act the obligation for providers of web browsers and providers of terminal equipment that define the rules for software applications collecting personal data through the use of that terminal equipment [‘operating systems’] to provide the technical means to allow data subjects’ to refuse a request for consentand exercise the right to object pursuant to Article 21(2) through automated and machine-readable means pursuant paragraph 1if the market offer for web browsers or operating systems is insufficient. Prior to the adoption of the delegated act, the Commission shall consult relevant stakeholders. The delegated act shall be adopted in accordance with the examination procedure referred to in Article 93(2).]	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.
	Connected Recitals: **(39)** 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 for direct marketing. Such means should follow the state of the art. They can be implemented in the settings of a web browser, in the terminal equipment where such terminal equipment defines the rules for software applications collecting personal data through the use of that terminal equipment (e.g. mobile phone operating systems) or in the EU Digital Identity Wallet as set out by Regulation (EU) 2024/1183, 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 Commission should be empowered to lay down obligations on web browsers or app stores when there is no uptake in terms of the provision of such technical interfaces by the market.]	
Article 88c -Processing in the context of the development and operation of AI		
	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 within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, except 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.	This article pushes the possibility to rely on legitimate interest as a legal basis to develop and operate AI systems. Problems: – **Slippery slope**: If legitimate interest is found for "*scraping the entire internet*" and any other available training data, for any purpose, without user consent, there is little other processing that would not be a "legitimate interest"; o The CJEU C-131/12, *Google Spain*, §81 already recognized the dangers associated with 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).

	Any such processing shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measure are in place in particular but not only 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 to provide data subjects with an unconditional right to object to the collection of their personal data. ' Connected Recitals: (27)[AI training based on legitimate interest] 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. This does not affect the obligation of the	○ Declaring "large scale data gathering" of any data a controller can physically access to be a "legitimate interest" for one technology would require very clear Recitals that would explain why such an approach would then not also be legal for any data broker, political operative or – **"Operation" goes far beyond "Training":** While arguments can be made that training data can be minimized, safeguards can be added and data may often be "washed away" in training processes, it is not clear at all why the "operation" of an AI system is automatically a "legitimate interest". We assume that "operation" (not being defined in the draft or the GDPR) would entail any "processing" of personal data via an AI system. ○ 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". – **Communication:** 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. ○ Information obligations in CJEU case-law: The CJEU considers in C-621/22, *Tennisbond*, § 49 that to rely on legitimate interest,

	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. (28) When the controller 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 non-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 ensuring data minimisation, providing enhanced transparency to data subjects, providing an unconditional right to object to the collection 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	the controller must comply with all of its obligations under the GDPR, including the transparency. 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, the CJEU also specified that the information must be given to the data subject at the time of the collection of the personal data. The current amendment does not reflect these information obligations; This can lead to interesting results. For example: The Italian SA has ordered OpenAI to inform people about the training via a "public awareness campaign", effectively buying TV ads, billboards and alike. – **Right to Object unrealistic in practice:** Linked to the lack of information and limited communication discussed above, it is entirely unclear how the "*absolute 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 timeframe applies to the objection. ○ Currently 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. ○ Furthermore, 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

	minimise risks resulting, for example, from regurgitation, data leakage and other intended or foreseeable actions.	the current draft does not seem to take these experiences (many dating back to the 1980ies) into account. ○ Even when a data subject would be able to "object", the controller would have to identify that persons' data in the dataset (or if "operation" is covered) of the trained AI model. This seems practically impossible, making the "absolute" right either a dealbreaker for AI training, or an unserious "safeguard". – **Necessity criteria in CJEU case-law:** in C-621/22 *Tennisbond* § 51, the CJEU set a strict interpretation for the necessity criteria: it considered that a sport club sending member's 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; – **Balancing under Art 6(1)(f)**: The new draft does not shed substantially more light into when an AI system can be legally trained or operated. ○ Expectations: 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 28 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; ○ Timing: The new wording 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). – **Minimization in CJEU case-law:** the CJEU stated (C-394/23, *Mousse*, § 42) that the systematic and generalised processing of personal data goes against the principle of data minimisation. In that case, it should have been limited to the processing of the data of "those customers who wish to travel in a night train or to receive personalised assistance on account of their disability". The same restrictive approach should be reflected in the provision; – **Broad scope of application:** in the given amendment, the GDPR refers to the extremely broad definition of AI from the AI Act. This broad definition was meant to have broad protections since many "traditional" processing activities would fall under it. Using this broad definition for an exemption would lead to an extremely broad privilege in the GDPR. It is very likely that this would go far beyond a "proportionate" limitation in light of the Charter; – ***Lex specialis* status:** It is unclear if this provision constitutes a *lex specialis* to article 6(1)(f) GDPR, as it refers to the provision but (i) where it says that the overriding interests or fundamental rights and freedoms of the data subject are those "*which require protection of personal data*", would that constitute a new „*condition*" in relation to the interests of the data subjects? It is also unclear if that aims to echo the new article 12 where controllers may refuse to grant access if the data subject pursues another purpose than purely data protection.

		(ii) the processing must be "*necessary for the interest of the controller*". How does that articulate with the requirement that the interest must be legitimate under Article 6(1)(f) GDPR? – **Compromising the GDPR's tech neutrality:** So far Article 6(1) is "tech neutral". Here a specific technology (AI) is for the first time (somehow) legitimized, 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; – **Data subjects' rights:** The proposed text seems to ignore the fact that the enforcement of data subject rights is at the moment not possible when it comes to AI technologies. More specifically when it comes to the right of access to training data, input and output, the controllers currently do not offer technological solutions to comply with data subject rights. Moreover, when it comes to the right of erasure, there are no guarantees that the data will not be reproduced by the AI system at any point in time; **See above on other notes on AI training generally and the proposed rules in Article 9(2)(k) above.** – **Sensitive data in CJEU case-law:** For sensitive data, in C-252/21 *Bundeskartellamt*, §89, the CJEU considered that when *en bloc* processing is in place without separation, the processing is prohibited if there is no legal basis according to Article 9(2) GDPR. The provision allows the *en bloc* processing of sensitive data, disregarding the CJEU position. Please also note our comments on the proposed Article 9(2)(k) above.

ePrivacy		
Article 4 - Security of processing		
1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented. 1a. Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least: - ensure that personal data can be accessed only by authorised personnel for legally authorised purposes, - protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and, - ensure the implementation of a security policy with respect to the processing of personal data.	[Agreement between CNECT and JUST reached on the principles but text still subject to fine-tuning between the DGs:] **DELETED**	Details unclear, not further investigated.

Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve. 2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved. 3. In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.	**DELETED**	

Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it. Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so. The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.	**DELETED**	

4. Subject to any technical implementing measures adopted under paragraph 5, the competent national authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification is to be made. They shall also be able to audit whether providers have complied with their notification obligations under this paragraph, and shall impose appropriate sanctions in the event of a failure to do so. Providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the competent national authorities to verify compliance with the provisions of paragraph 3. The inventory shall only include the information necessary for this purpose. 5. In order to ensure consistency in implementation of the measures referred to in paragraphs 2, 3 and 4, the Commission may, following consultation with the European Network and Information Security Agency (ENISA), the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC and the European Data Protection Supervisor, adopt technical	**DELETED**	

implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements referred to in this Article. When adopting such measures, the Commission shall involve all relevant stakeholders particularly in order to be informed of the best available technical and economic means of implementation of this Article. Those measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 14a(2).		
Article 5(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	[Agreement between CNECT and JUST reached on the principles but text still subject to fine-tuning between the DGs:] 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	***Note: See above Article 88a GDPR on the processing of "personal data" for most of the relevant problems.*** Problems: – **Stricter rules for non-personal data:** The much stricter protections under Article 5(3) ePrivacy would still apply to any non-personal data. This would mean that non-personal data is protected to a higher degree than personal data.

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.	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 does not apply where personal data is processed on or from terminal equipment in accordance with Article 88a of Regulation (EU) 2016/679.** **Connected Recitals**: (40) [Approach agreed, text still being fine-tuned] [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 information in or from the terminal equipment does not constitute and does not result into processing of personal data.] (41) Article 4 of Directive 2002/58/EC should be repealed. Article 4 of Directive 2002/58/EC sets requirements for providers of publicly available electronic communications services as regards safeguarding the security of their services and notification requirements. Subsequently, Directive (EU) 2022/2555 has set new	– **Conflict with limitation of Charter Rights:** It would be hard to argue under Article 8 and 52 of the Charter, that the legislator "had to" protect personal data less than non-personal data. – **Jurisdiction problem further escalated:** There is a longstanding issue that for the setting of cookies or the reading of data from a terminal Telco Regulators under ePrivacy are often in charge, while for personal data (under Article 8(3) of the Charter) SAs must be in charge. This splits cases and investigations. o The jurisdiction for "*access to the terminal equipment*" would continue to be split between GDPR SAs, just now for processing of personal data and other Regulators (often Telco Regulators) for non-personal data. o In addition, a rather complex investigatory step (find out if in the individual case "*personal data*" was processed, which controllers regularly deny) has to be carried out just to know which regulator (!) is in charge of a complaint. o The rights and systems for complaints under ePrivacy and GDPR are also different, leading to problems (e.g. Telco Regulators may only treat the complaint as a "*petition*", which does not allow the data subject to appeal the outcome and make the point that it actually *did* concern personal data and *should* have been sent to the SA, because it may lack party rights). o This split was exactly an aim to overcome in order to streamline compliance and enforcement, now the procedural overhead resulting from this "split" may even increase.

	requirements as regards cybersecurity risk-management measures and incident reporting for those providers. In order to reduce overlapping obligations for entities in the electronic communications sector, Article 4 of Directive 2002/58/EC should be repealed. As regards the security of processing of personal data pursuant to Article 4(1) and (1a) of this directive and the notification of personal data breaches pursuant to Article 4(3) to (5) of Directive 2002/58/EC this directive, the Regulation (EU) 2016/679 already provide for comprehensive and up-to-date rules. These rules should therefore apply to providers of publicly available electronic communication services and providers of public communications networks, thereby ensuring that one regime applies to the controllers and processors.	