PROCEED WITH CAUTION:

High risk flexibilities in the General Data Protection Regulation

European Digital Rights | 20 Rue Belliard, 1040 Bruxelles, Belgium | Tel. +32 2 274 25 70 | www.edri.org

EDRi analysis on the most dangerous flexibilities allowed by the General Data Protection Regulation (*)

General Note on divergences:

One of the main reasons for adopting the main Data Protection Directive (DPD) in 1995 was that the different data protection laws in the Member States (and the absence of any such laws in some of them) hampered the Single Market. The aim of the 1995 DPD was to create a largely harmonised data protection system throughout the EU (and the EEA). However, reviews of the laws in the Member States (MSs) adopted to implement the directive showed that, it had in many respects, failed to achieve harmonisation: there were still many, often major, differences between the laws in the MSs.

Despite this experience, the GDPR contains **a large number of provisions that allow the Member States to set the rules in many important contexts.** These divergences can lead to differences in the protection of personal data, which would create unfair competition and could hamper the Digital Single Market. More importantly, the divergences could create **different levels of protection for EU citizens.** Consequently, these divergences may be used by MSs as wiggle room to lower the bar for the protection of citizens´ data. The spirit of the GDPR is completely the opposite, as it aims at improving the single market and harmonising the level of data protection for all people living in the EU.

The flexibilities in the Regulation are to be found in a large number of articles and recitals, effectively creating a sort of hybrid between a Regulation and a Directive. One major issue for the implementation of the GDPR will be who is responsible for issuing advice and guidance on the multiplicity of general or unclear terms used in the articles – the national authorities, or the new to-be-set-up European Data Protection Board (EDPB); or when does the consistency mechanism (the process to ensure consistency of application throughout the Union) kick in, and what about cases where there maybe a mixture of existing national-only legislation (e.g. employment or trade union law), and cross-border applications. Or will all these be decided eventually by the courts?

(*) This is the short version of a more comprehensive analysis which can be found **here**. In this document, we have only included those flexibilities that pose the most serious problems, especially in relation to the online environment and the Digital Single Market.

CHAPTER 2: PRINCIPLES		ANALYSIS AND SUGGESTIONS FOR INTERPRETATION
Article 6(4). Related to Recital 50	Further processing for "incompatible" purposes	**Problem: assessment of compatibility left to the controller; criteria for assessment are vague; countries may interpret them differently** **EDRi suggestion:** the assessments of the controllers on "compatibility" should be subject to review by the relevant DPA ; in relation to any cross-border activities, the views of the DPA in question should be subject to the cooperation-, mutual assistance- and consistency mechanisms. For important or regular types of "incompatible" processing (e.g. medical data gather by general practitioner to be sent to a private medical investigative clinic for a nation-wide research), the EDPB should issue much more specific guidance and rules.
Articles 9(2)(h), 9(2)(i) and 9(4) **Related to recitals 52-54**	Processing of sensitive data for health purposes	**Problem:** Member States may provide for specific rules to allow processing of individuals' data for broadly-formulated healthcare and related purposes without consent, including via contracts with a health professional. **The safeguards are vaguely defined, so they will end up being different; as "applicable law" rules are missing in this Regulation, it could lead to forum shopping in the health-care and products single market.** **EDRi suggestion:** We suggest implementing this article in a way that the applicable law is clearly stated in Member States and that EDPB level guidelines and standards regarding DSM use of health data/products are issued.
Articles 9(2)(j) & 89 **Related to recitals 53-54**	Processing of sensitive data for archiving purposes and, historic and scientific research	**Problem:** Public interest is not defined, so the scope of this provision is left to each Member State to define. In practice, this could be affected by political priorities; there is a significant risk of highly sensitive data being obtained also for commercial "research" purposes. There is also a risk of forum shopping. **EDRi suggestion:** The EDPB should issue common guidance as to what would constitute public interest in such cases; we suggest implementing this provision by not including commercial research purposes as an exception to consent, even if it is done in the (defined) public interest.

CHAPTER 3: RIGHTS OF THE DATA SUBJECT Section 2: Information and Access to Data		ANALYSIS AND SUGGESTIONS FOR INTERPRETATION
Article 14(5)(c) Related to Recital 62	Exception to right to information when data are not obtained from the data subject	**Problem:** Individuals in one EU country buying goods or services online from companies in another will be left in the dark about possibly extensive, and possibly excessive, disclosures of their data to a public or even private entity **EDRi suggestion:** National DPAs must approve the application of this article, that the disclosure of the data to certain bodies is not only expressly laid down in EU or national law but that that the measures to protect the data subject are indeed appropriate

CHAPTER 3: RIGHTS OF THE DATA SUBJECT (Section 4: Right to Object and Automated Individual Decision Making)		ANALYSIS AND SUGGESTIONS FOR INTERPRETATION
Article 22(2)(b) **Related to Recitals 71 & 72**	**Automated individual decision making, including profiling**	**Problem**: This exemption allows completely secret automated profiling which can significantly affect the data subject, under MS or Union law and with undefined safeguards **EDRi suggestion: We encourage Member States to not implement (or derogate if they exist) such legal authorisations for processing done by private sector controllers and specifically in commercial contexts without informing the data subject**. At the very least, MSs should be required to inform the EDPB and the public of the way in which they use the exemptions. Much more detailed guidance should be provided on what exemptions are, and are not, acceptable, in particular in the Digital Single Market. We suggest that automated processing under Article 22(2)(b) is only conducted following guidance issued by the EDPB on common safeguards of data subjects' rights. Regarding profiling done by public authorities, such activity should be done after the national DPA has provided a positive opinion on the purpose and safeguards of such measure.
Article 23 **Related to recital 73**	**Restrictions on data subjects' rights**	**Problem:** The article authorises member states to **restrict by law the application of data subject's rights** for purposes of national security, defence, public security, the prevention or investigation of crimes, “other important objectives of general public

		interests”. **The application of the exemptions remain largely discretionary and almost entirely in the hands of the Member States.** Moreover, under this provision Member States can adopt domestic exemptions that directly impact on the processing of personal data in transnational and online contexts: **the provision is not limited to exemptions for the benefit of public authorities only, but can also be used to exempt private-sector controllers (companies)** from the normal requirements relating to data subject rights, e.g., in relation to online fraud detection by banks. The scope is significantly broader than the eqivalent article from the 1995 Directive. **<u>EDRi suggestion:</u>** We suggest that EDPB and DPAs issue guidelines on how these restrictions need to be (strictly) interpreted in order to allow that these exceptions are only for the pursuance of a demonstrable legitimate aim, genuinely achieve objectives of general interest and that they are in compliance with the principles of legality, necessity and proportionality.

CHAPTER 4: CONTROLLER AND PROCESSOR Section 1: general obligations		ANALYSIS AND SUGGESTIONS FOR INTERPRETATION
Article 26(1) **Related to Recital 79 (cf. also 110)**	Joint controllers	**Problem: this provision lets companies working together on processing personal data make their own arrangements as to their responsibilities under this Regulation, with no formal requirements. This provision grants excessive freedom to joint controllers** (which are increasingly common in the increasingly complex chains of companies involved in commercial activities, in particular online) to choose “arrangements” for themselves that place their operations under the (for them) least demanding regime. This could threaten the Digital Single Market by creating a “race to the bottom”. **EDRi suggestion:** In order to counter this serious risk, the stipulation that the “arrangements” should reflect actual divisions of responsibility rather than create evasions from strict rules in some MSs, should be strongly and firmly enforced by the DPAs in the Member States. This applies in particular in relation to multinational corporations operating online , especially by means of the cooperation-, mutual assistance- and consistency mechanisms in the Regulation. .
Article 28(3)(a)&(g) **(Cf. also Articles 29, 32(4) & 38(5))** **Not related to any recital**	Processor ordered to process contrary to instructions by the controller as required by domestic laws	**Problem:** Some Member States have laws that impose obligations on processors (and controllers) in violations of ECHR and the EU Charter of Fundamental Rights, particularly in relation to state surveillance. **EDRi suggestion:** We suggest that DPAs use all means at their disposal to prevent a watering-down of the GDPR protections and, where there are not such laws yet in place, **Member States should review their laws and practices to ensure they are in compliance with applicable human rights standards**. DPAs to review the scope of

		obligations of processing imposed by national laws; and the EDPB to provide common guidance.
Article 29	None (in particular not addressed in Recital 81)	**Problem:** This provision essentially repeats the stipulations in Article 28(3)(a) & (g), discussed above, with regard to "any person acting under the authority of the controller or of the processor who has access to personal data**". It effectively states that when EU law or the law of a MS requires such a person to process the data other than as instructed by the controller or the processor, e.g., to disclose the data to a law enforcement- or national security agency in the MS, or indeed to transfer or disclose the data to a third country or international organisation; or not to erase the data at the end of a processing contract, the person concerned must do as instructed by the MS, irrespective of the will of the controller or the processor (or the purpose-limitation principle).** The conclusion must therefore be the same: **this constitutes another *carte blanche* that fails to protect EU data subjects against the kind of "generalised access" to their data by EU MSs' agencies that the CJEU found in relation to the US agencies to impinge on the very "essence" of the right to privacy. It too is unacceptable.** **EDRi suggestion:** We suggest that DPAs carefully review such national laws in order to prevent unlawful access to/disclosure orders.

CHAPTER 4: CONTROLLER AND PROCESSOR Section 2: data security		ANALYSIS AND SUGGESTIONS FOR INTERPRETATION
Article 32(4)	Security of processing	**<u>Problem</u>**: This provision is essentially a repetition of Article 29. However, it is notable that here it is contained within the section and first article dealing with data security (Section 2, Article 32). This can only mean that the **legal duties in mind here relate in particular to IT security measures – or rather, to legally imposed duties to by-pass or undermine the security of the processing in question, e.g., the compulsory installing of "back doors" into databases or communication systems**. If this is indeed what the provision seeks to expressly allow to be done – indeed requires to be done – whenever that is provided for (required) under the domestic law of a MS, **it again constitutes an unacceptable *carte blanche* allowing for interferences with EU data subjects' privacy- and data protection rights, in violation of the Charter**. It should also be noted that the Dutch government specifically issued a statement regarding the importance of not undermining cryptography standards and the prohibition of imposing back doors unto software or hardware. This clause could undermine this statement and would, if used by other MSs, harm the Digital Single Market. **<u>EDRi suggestion:</u>** We suggest that DPAs revise related existing laws to prevent a watering-down of the GDPR protections and that, in case there are not such laws in place yet, Member States refrain from creating them and thus from violating the Charter of Fundamental Rights.

CHAPTER 5: TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS		ANALYSIS AND SUGGESTIONS FOR INTERPRETATION
Article 46(2)(a) **Related to Recital 108**	Transfers subject to appropriate safeguards provided	**<u>Problem:</u>** This provision appears to constitute a *carte blanche* through which Member States can self-authorise transfers of any personal data, for any purpose, to any "public authorities or bodies", in any country without adequate data protection

	for in legal instruments between public bodies	**EDRi suggestion:** These “legally binding and enforceable instruments” between authorities should be certified by DPAs and supervised by the EDPB before they are put in place.
Article 48	Transfers or disclosures not authorised by Union law (the so-called “Anti-NSA Clause”)	**Problem:** This provision clearly allows for disclosures of personal data to third countries based on international agreements which could be not only secret but also In manifest breach of the EU Charter of Fundamental Rights. **EDRi suggestion:** We suggest that Member States implement this measures passing provisions to ban the use of “gagging orders” and secret international agreements when implementing such disclosure orders. **Additional measures to ban indiscriminate hidden disclosures of personal data to foreign agencies and courts should be suggested by the EDPB** to avoid the loopholes that this provision creates.
Article 49(1)(d), read together with (4) **Related to Recitals 111&112**	Derogations for data transferred for important reasons of public interest	**Problem:** effectively another *carte blanche* handed to the Member States, allowing them to circumvent the otherwise seemingly strict rules on data transfers. **EDRi suggestion:** We suggest that Member States apply this derogation strictly for the kind of “public interests” examples listed in the Recital 112 of this Regulation (e,g competition authorities, tax and customs, financial supervision).

CHAPTER 6: INDEPENDENT SUPERVISORY AUTHORITIES Section 2: competence, tasks and powers		ANALYSIS AND SUGGESTIONS FOR INTERPRETATION
Article 55(2) read with Article 6(1)(c)& (e) and Article 56 **Related to Recital 128**	Competence in relation to cross-border processing to comply with a legal obligation, for a public interest task, or under official authority	**Problem:** With this provision, the DPA of the MS that imposes such processing to comply with “legal obligations” or a public interest task, or under official authority need not even inform the other DPAs of such handing over of data. It is unclear whether the cooperation-, mutual assistance- and consistency mechanisms apply in such cases, since they all hinge on the “lead authority” working closely with the other DPAs concerned. If there is no lead authority, how is this to be achieved? **EDRi suggestion:** We suggest that DPAs of all MSs involved are informed of any handling of data enforced under this provision.

CHAPTER 7: CO-OPERATION AND CONSISTENCY Section 1: co-operation		ANALYSIS AND SUGGESTIONS FOR INTERPRETATION
Article 61(4)b) **(See Recitals 133 – 135)**	Refusal of cooperation and mutual assistance	**Problem:** This provision stipulates that a DPA in one EU MS may refuse to comply with a request for assistance from a DPA in another MS if “compliance with the request would infringe” the law of the former MS. Neither the article nor the recitals clarify when and how this provision will apply, or give any illustrations or examples. **The article is problematic if read in the light of Article 55(2)** It may be feared that these exemptions will be applied in particular in relation to national security issues. Thus, if a DPA in one MS feels that the rights of data subjects in that MS may be affected by, say, disclosures by private companies in another MS to the national security agencies of that other MS (or if a data subject or association complains about this), then the DPA in the other MS will be prevented in cooperating in the investigation, if the law in that latter MS prohibits this or essential elements of it such as the disclosure of any information relating to the relevant matter (e.g., again, national security). **EDRi suggestion:** The new **European Data Protection Board should issue guidelines urgently** on how this provision is to be applied; and in that it should consult civil society, including freedom of expression- and digital rights groups.

Chapter 9: PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS		ANALYSIS AND SUGGESTIONS FOR INTERPRETATION
Article 85 **Related to Recital 153**	Processing of personal data and freedom of expression and information	**<u>Problem:</u>** Article 85(1) stipulates that MSs must (“shall”) reconcile the right to data protection and freedom of expression. **<u>EDRi suggestion:</u>** The new **European Data Protection Board should issue guidelines <u>urgently</u>** on how this provision is to be applied; and in that it should consult civil society, including freedom of expression- and digital rights groups.
Article 89 **Related to Recitals 156 – 163**	Safeguards and derogations for the processing of personal data for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes	**<u>Problem:</u> Article 89(1) and Article 9(2)(j) create dangerous loopholes in the protection of personal, and especially sensitive, data.** Presumably, the reference in Article 89(1) to the need for “appropriate safeguards” means that the actual safeguards adopted by the different MSs can be challenged in the courts, including ultimately the CJEU. **<u>EDRi suggestion:</u>** It will be crucial for the new **European Data Protection Board to issue clear and strict guidance on these issues as a matter of <u>great urgency.</u>**

This document was prepared by:

EDRi

PROTECTING DIGITAL FREEDOM

fipr

accessnow

PRIVACY INTERNATIONAL

PANOPTYKON FOUNDATION

BITS OF FREEDOM

VERDEDIGT DIGITALE BURGERRECHTEN