Tasks and Obligations

Conditions for Consent (Article 7)

EDRi welcomes the fact that Article 7(1) places the burden of proof on the controller, as well as introducing safeguards to verify the validity of the consent in the cases of significant imbalance between the position of the data subject and the controller.

General Obligations

As a general remark, the exceptions provided to SMEs regarding compliance with the Regulation are acceptable, provided that citizens have the same protections regardless of the size of the enterprise or body that is processing their personal data. The essence of the right may not be diluted and, therefore, it should be made explicitly clear that such exceptions apply only to Chapter IV and not the Regulation as a whole.

Responsibility of the Controller (Article 22 & 28)

EDRi welcomes that Article 22 (paragraphs 1 and 3) obliges the controller to ensure and demonstrate compliance, and sees this as an effective way or ensuring accountability on the part of the controller. To add further clarity to Article 22(2), we suggest adding a reference to Article 11 on transparent information and communication. Furthermore, it should be made clear in the Regulation that the principle of accountability shall not be limited to the elements listed in Article 22(2).

In line with the provisions in Article 11, Article 22(3) should be strengthened to include that such verifications ensuring the effectiveness of measures in (1) and (2) must be done transparently and made publicly available. Such “transparency reports” should include the information referred to in Article 22(1) and (2). EDRi also questions the ability of verifications to be truly independent if they are carried out by internal auditors.

In order to maximise efficiency and effectiveness, industry sectors should cooperate with supervisory authorities to harmonise such compliance documentation, creating economies of scale for business and predictability and transparency for citizens and supervisory authorities.

Data protection by design and by default (Article 23)

EDRi welcomes the inclusion of a separate Article on data protection by design and by default, however, the current drafting of this article lacks a clear definition and practical applications. In order to operationalise these obligations, we strongly suggest the following changes:

Firstly, include a clear definition of data protection by design in recital 61. This could say for example, “Data protection by design is the process by which data protection and privacy are integrated in the development of products and services through both technical and organisational

measures." This definition should be further specified by adding *1(a) Technical measures*, which refer to the physical design of products, such as hardware and software; and *1(b) Organisational measures*, which include external and internal policies, current best practices.

Similarly, the definition of privacy by default (paragraph (2)) also needs to be more specific and include references to both the technical and organisational aspects. We therefore suggest the same delineation of 23(*2)*(a) *Technical measures*, referring to data settings in hardware and software by companies; and *2(b) Organisational measures*, referring to privacy protections available to the data subject. In this case, the most privacy protective option should be the basis if it is enough to achieve the specific and limited purposes of the collection of data. This includes, for instance, that controllers do not prohibit data subjects from using pseudonyms on their services unless strictly necessary.

On controllers, joint controllers & processors (Articles 24-29)

EDRi agrees that in situations where a controller defines the processing of personal data jointly with others (Article 24), it should be compulsory that they make arrangements between them.

Data Security

Security of processing (Article 30)

Article 30 states that whenever there are risks inherent in the processing of personal data, both the controller and the processor must first evaluate them and then take appropriate security measures. However, specific rules for how to determine the level of security are needed. To this end, EDRi recommends including a reference to Article 33 in 30(2) when referring to "an evaluation of the risks".

As the Article currently stands, it is not clear whether the controller or processor, or both equally, have responsibility. The Article should emphasize that the overall responsibility lies on the controller (as specified in Article 22 and 26).

Data Breach Notification (Articles 31-32)

EDRi is pleased that the Regulation includes a provision on mandatory data breach notification to the data subject (Article 32(1)), however the phrase 'likely to adversely affect' seems too vague and should be further specified. Detailed criteria and requirements are needed for establishing what constitutes a "data breach" and what threshold requires notification. If the Commission chooses to specify this in delegated acts (Article 32(5)), they should be adopted at or before the entry into force ofthe Regulation, to avoid a legal void, however temporary this may be.

As the Regulation seeks to establish greater accountability and transparency, we also suggest that notifications to the data subject should extend the current scope of "at least the information and recommendations provided for in points (b) and (c) of Article 31(3)", to also cover points (a), (d) and (e) of Article 31 (3).

Finally, while expeditious notification of data breaches are needed, a 24-hour time limit (Article 31(1)) might be difficult to realistically implement, and could potentially undermine the effectiveness of these provisions. Considering that this provision will apply to many different types of controllers, from small companies to large enterprises, one time limit may not be appropriate in all cases. We

therefore suggest extending this to 72 hours.

Data protection Impact Assessment (DPIA) (Article 33)

Article 33(2)(a) provides a list of processing operations that includes ambiguous phrases such as "significantly affect the individual" 33(2)(a), or "on a large scale" 33(2)(a),(b), that may obscure the scope of the DPIA.

EDRi recommends stating more clearly that the exception for carrying out a DPIA as it is made in Article 33(5) only applies if an equivalent assessment has been made in the legislative context.

Data Protection Officer (DPO) (Articles 35-37)

EDRi sees the increased specifications and the mandatory designation of a data protection officer as an improvement from the Directive 95/46/EC, and understands that the DPO's ability to perform his/her job (including informing and advising the controller or processor of their obligations, and to internally oversee application and compliance with the Regulation) requires independence, as indicated in Article 36(2). However, it should be made clear that the DPO is not the only person involved in ensuring compliance with the Regulation (think for example, of Article 23 which introduces obligations that data protection compliance throughout the entire DNA of a company, organisation or body).

To ensure greater clarity, we suggest making explicit reference to the rights mentioned in 37(1)(c), including Articles 23 and 22, 30-32, Articles 11-20.