Executive summary

EUROCHAMBRES welcomes the Commission’s initiative to review the EU data protection legislation – a reform is absolutely necessary in order to keep up with the changes brought about by globalisation and technological and scientific progress. The Chambers support the Commission’s objectives to modernise and further harmonise the EU legal framework on personal data protection, as well as to enhance legal certainty and reduce red tape. However, the Chamber network is not convinced that the latter goals were attained with the current proposal for a General Data Protection Regulation. While removing some of the bureaucratic requirements, the draft Regulation imposes a number of new obligations on controllers and processors, which are far more burdensome than the existing legal duties. Moreover, the new data subjects’ rights introduced by the proposal might be very hard to put into practice and might hinder innovation and growth of the digital economy.

EUROCHAMBRES believes that a better balance needs to be struck between the protection of fundamental rights and businesses’ needs to enable them to operate and innovate in this highly regulated environment.

In order to achieve this better balance and to make the data protection legislation more flexible and hence future-proof, the Chamber network recommends adequately modifying the following issues:

- The number of delegated acts and implementing acts must be reduced
- Respecting the principle of technological neutrality is crucial
- The current definition of consent should be retained
- Information obligations of controllers towards data subjects are too burdensome
- The right to be forgotten might not be practically feasible and it would be hard to reconcile it with the freedom of expression
- The right to data portability lacks clarity as to how it would be implemented
- The right to object to the processing of personal data should be clarified
- Draft provisions on profiling might have adverse effects on sectors such as healthcare, banking and retail
- Certain provisions will prove excessively costly and burdensome for controllers and processors (especially SMEs)
- The 24-hour deadline to notify a personal data breach to the supervisory authority is too short
- Appointing a data protection officer should not be obligatory
- **Transferring personal data beyond the EU borders** should be further simplified
- **Penalties** for infringements of data protection rules are disproportionately high
- More **transitional provisions** are needed
- No need to allow organisations to bundle claims

**Detailed comments**

1. **There should be fewer delegated and implementing acts**

EUROCHAMBRES believes that the powers granted to the Commission by the draft Regulation are far too wide and in effect it would impair legal certainty and predictability.

There are over 20 provisions that give the Commission the authority to adopt delegated acts, in accordance with Art. 290 TFEU. The issues to be regulated by the Commission range from the criteria for lawfulness of processing data on the basis of the legitimate interests of the controller (Art. 6(5)) to updating the amounts of the administrative fines for non-compliance with the Regulation (Art. 79(7))

Under the draft Regulation, the Commission also has significant implementing powers for specifying certain forms, formats, procedures and technical standards, e.g. as regards data portability, security of processing and privacy by design and by default. Some which would be best left to self-regulation and standards agreed by the business community.

Regulating so many issues by delegated and implementing acts undermines legal certainty and predictability for businesses, as they cannot be sure what exact rights and obligations are. Given the significant fines for non-compliance with the Regulation, any uncertainty should be avoided.

Moreover, under Art. 290 TFEU, the Commission can only adopt delegated acts regarding non-essential elements of a legislative act, and the objectives and content of a delegated act should be explicitly defined in a legislative act. EUROCHAMBRES believes that at least some of the delegated acts foreseen by the draft Regulation pertain to essential issues, e.g. lawfulness of processing on the basis of the legitimate interests pursued by the controller, criteria for establishing a data breach, and updating the amounts of administrative fines. Also, in many cases the content of delegated acts is not sufficiently defined.

Therefore, the number of delegated and implementing acts should be significantly reduced and they should only concern minor, non-essential matters. Where the acts are retained, it should be announced when they would be adopted.

---

1 Other matters to be regulated by the Commission by delegated acts include among others: (i) criteria, conditions and safeguards for the processing of the special categories of data (so-called sensitive data), (Art.9(3)); (ii) criteria and conditions for safeguarding the data subject’s legitimate interests in cases of profiling (Art. 20(5)); (iii) criteria and requirements for privacy by design and data protection by default measures (Art. 23(3)); (iv) criteria and requirements for privacy by design and data protection by default measures (Art. 23(3)); (v) criteria and requirements regarding the obligation to maintain documentation of all processing operations (Art. 28(5)); (vi) criteria and conditions for the technical and organisational measures to ensure an appropriate level of security, including determinations what constitutes state of the art (Art. 30(3)); (vii) criteria and requirements for establishing a personal data breach (Art. 31(5)); (viii) criteria and conditions for the especially risky processing operations, where a data protection impact assessment is necessary (Art. 33(6)).
Also, if self-regulation or agreed standards cannot be used, the business community should be involved in the elaboration of such acts to ensure that the rules are economically and technically practicable from businesses’ point of view.

2. **The principle of technological neutrality is essential**

The Chamber network would like to underline that the future legislation (including any delegated and implementing acts) must be technologically neutral so as to ensure its future-proof character, encourage innovation and progress of all new technologies, industry trends and services (e.g. cloud computing, mobile technology and mobile applications, geo-location, face recognition).

3. **The current definition of consent to personal data processing should be retained**

The draft Regulation introduces certain new requirements regarding data subject’s consent to the processing of their data, i.e. the consent has to be explicit, the controller bears the burden of proof that the consent was obtained, and the consent is not a valid basis for data processing if there is a significant imbalance between the position of the data subject and the controller. Under the current regime (Directive 95/46/EC), an explicit consent of the data subject is only necessary for the processing of sensitive data.

Such rules will be very costly and burdensome for controllers and processors, because in many cases a change of existing business practices and procedures will be necessary. EUROCHAMBRES considers the requirements of explicit consent and burden of proof excessive. In our opinion the explicit consent requirement should only apply in case of sensitive data processing.

Furthermore, the term “significant imbalance” is very vague and adds to legal uncertainty. In view of large financial sanctions for non-compliance with the Regulation, such an unclear provision might even put a business at risk. Therefore, the Chamber network recommends that this provision be deleted.

4. **The information obligations of controllers should be simplified and reduced**

Just as the new requirements regarding consent, the newly introduced information obligations of controllers towards data subjects and supervisory authorities are excessive and would entail high administrative expenses. The Chamber network believes that these rules, while a burden on controllers, will not necessarily benefit the data subjects. These are much more likely to read a simple, clear and brief note than an excessively long and complicated one.

5. **The practical feasibility of the right to be forgotten and its impact on the freedom of expression should be reconsidered**

The right to be forgotten – i.e. to have one’s personal data erased and not further disseminated – raises significant doubts as to its practical implementation, costs and potential impact on Internet business models. It is particularly difficult to imagine the functioning of this right in the online environment, and especially in case of social networking.

First of all, it is often impossible for a controller to identify all the data concerning a particular person, for instance when it was provided by a third party. Thus, erasing all data on a particular data subject might simply not be feasible. Any proposal should be limited to data held or direct control by the controller.

The obligation of the controller to inform third parties processing data made available by the controller that a data subject has requested erasure of their data might also not be possible. Controllers (especially in the online environment) are not in a position and should not be obliged
to keep track of all the third parties that might get hold of data that is publicly available or available to them (who are potential data processors). Such an obligation would entail enormous costs and a necessity to process even more personal data.

The right to be forgotten should be limited to data users themselves have submitted and not data generated when using a service (such as error messages or operational statistics) or data to which the company has other rights. There should also be a possibility to, for a reasonable duration, save data for reactivation for a user account at the request of the user.

The effect of this right on the freedom of expression and freedom of communication has to be analysed in more detail. Under the current draft, the controllers would have to make complex decisions on balancing the right to be forgotten against the freedom of expression, and whether specific data ought to be erased or not. In case when an online service involves a possibility to send and receive correspondence to and from other users, such other users should be allowed to keep a copy of correspondence even if one other party requested erasure of their data. It should also be noted that the draft Regulation provides no guidance in this respect.

Therefore EUROCHAMBRES recommends that the right to be forgotten be reconsidered in the light of the issues stated above, and deleted or amended accordingly.

6. The practical implementation of the right to data portability should be better explained

EUROCHAMBRES has serious doubts as to how the right to data portability could be carried out in practice. Not all data can be easily put “in a structured and commonly used format”. We also oppose the Commission’s power to set technical standards for porting data as it could impede innovation – we believe that self-regulation would be a better approach.

Moreover, the relationship between this right and the certain intellectual property rights, especially regarding the legal protection of databases, should be made clear.

7. The right to object to the processing of personal data has to be clarified

The exact scope of the right to object to the processing of personal data is unclear, especially when compared to the right to be forgotten. First, the grounds for objecting to data processing have to relate to a data subject’s “particular situation” – it is a very vague term, which makes it impossible to determine when this right could be exercised.

Second, it appears that the right to object is somehow contained within the right to be forgotten. According to Art. 17(1)(c), one of the grounds on which the right to be forgotten can be exercised is the data subject objecting to the processing of their data pursuant to Art. 19. Consequently, the effects of exercising the two rights should be identical. However, while the right to be forgotten potentially applies to all data processing cases mentioned in Art. 6(1), the right to object can only be used when personal data is processed based on (i) vital interest of a data subject, (ii) public interest, and (iii) legitimate interest pursued by the controller and when the aforementioned “particular situation” criterion is fulfilled. In consequence, establishing in which situations one can exercise the right to object, or the right to be forgotten, or both, is very complicated. It would prove confusing for data subjects and businesses alike.

EUROCHAMBRES recommends that the right to object be clarified, particularly as to its relationship with the right to be forgotten. Its scope of application should also be made clear, and it should be limited to very specific and well-defined cases.
8. The draft provisions on profiling need to be reviewed to ensure that they do not negatively affect sectors such as healthcare, banking, and retail

The draft provisions on profiling must be carefully reviewed and its potential effects have to be examined cautiously. It should be remembered that predictive data analysis techniques are used in a broad range of sectors, for example in relation to employment (e.g. assessment tests), creditworthiness and healthcare. In many cases predictive analytics is used for valid reasons, e.g. fraud detection, research activities, improvement of services, detection of health risks, marketing, etc. EUROCHAMBRES suggests amending the provisions on profiling so that such predictive data analysis techniques can be used for legitimate reasons such as those mentioned above.

The exact wording of this provision (“right not to be subject to a measure” based on profiling) suggests that a data subject may object to profiling even when it is permitted by law. In our opinion this should not be the case, and the wording needs to be modified accordingly.

9. The costly and burdensome obligations have to be adequately reduced

Although the goal of the draft Regulation is to reduce red tape, the new provisions arguably impose even more administrative obligations on controllers and processors. While the general obligation to notify a relevant data protection authority (DPA) about processing operations is abolished by the proposal, the new duties include retaining extensive documentation on data processing and carrying out data protection impact assessments. Such obligations will no doubt be extremely costly and burdensome for controllers, and are clearly incompatible with the objective of reducing administrative duties.

It should also be noted that in the above cases the Commission is empowered to adopt delegated acts and implementing acts, e.g. on standards forms for the documentation; on criteria and requirements for the documentation; and on criteria of specifically risky situations where a data protection impact assessment is necessary. It is therefore impossible to properly assess the scope of these obligations, which might prove even more excessive once spelled out by the Commission.

EUROCHAMBRES recommends that at least some of these obligations be lifted. For instance, controllers should have the choice between notifying the DPA about their data processing operations and maintaining detailed documentation of processing operations. The duty to carry out a data protection impact assessment should be limited to very specific situations. Also, as we stated earlier (point 2), the Commission implementing powers should be limited to non-essential matters only.

10. The rules on notification must be more flexible and harmonized

In the opinion of EUROCHAMBRES, the 24-hour deadline to notify a personal data breach to the DPA is an inadequate approach. Immediately after discovering a data breach, controller’s efforts are concentrated on identifying the nature of the breach, stopping the data leak and assessing its extent and possible consequences for data subjects. Only once this information is complete will the controller be in a position to exhaustively inform the DPA of the data breach and its outcome. It is also likely that in many situations it will be more important to inform the data subject before the supervisory authority (cf. Article 32.1).

The definition of a personal data breach may be too wide to be useful. It now covers almost all kinds of incidents. Data protection risks and issues may vary significantly over time and depend on what kind of data on who are concerned. There are data security rules for data protection in directive 2002/58/EC (Directive on privacy and electronic communications), there is a need to harmonize these rules.
The proposal has a 24 hour rule for notification of personal data breach is not in directive 2002/58/EC. Therefore, such a short deadline would hinder rather help dealing with the breach effectively. The Chamber network suggests that this rule is made much more flexible, the deadline be deleted or at least significantly prolonged.

11. **The choice between appointing a data protection officer and notifying the data protection authority should be retained**

Appointing a data protection officer should not be obligatory. Under Directive 95/46/EC, Member States are given the choice of requiring controllers either to notify the DPA about the data processing operations or to appoint a data protection officer (Art. 18(2) of the Directive). EUROCHAMBRES is of the opinion that the two options should be retained in the new Regulation as several Member States adopted the notification system and it is functioning well in those Member States.

Moreover, if a Member State opts for the data protection officer (DPO) system, the obligation to appoint one should not be dependent on the size of an enterprise, but on the character of its core business activities. Only the companies for which processing personal data constitutes their core activity should be required to appoint a DPO.

12. **Transferring personal data beyond the EU borders should be further streamlined**

EUROCHAMBRES believes that the international data flows are crucial to the growth of the digital economy. The global nature of the Internet entails the global reach of cross-border data transfers, and such transfers should not be unnecessarily obstructed. European businesses must be able to export data to third countries in order to ensure their competitiveness and presence in foreign markets. While we welcome many of the proposed rules that facilitate data transfers to third countries – e.g. explicitly recognizing binding corporate rules (BCRs) as a valid ground for data transfers, no prior authorisation requirement when making use of approved BCRs and standard data protection clauses – in certain cases we see the need to further simplify and clarify the rules and procedures governing cross-border data flows.

The procedure and criteria for adopting an adequacy decision should be streamlined. Because of the process’ complexity and the huge effort needed to analyse all the elements concerning a third country’s laws listed in the proposal, taking an adequacy decision will be excessively time-consuming. Since 1995 when the Data Protection Directive was introduced, the Commission has only adopted 12 such decisions. Therefore the new rules should put forward a simplified procedure and assessment criteria.

It also has to be clarified that in the event where the Commission finds that the level of protection in a given country or sector is inadequate, the transfers are still permitted by the way of appropriate safeguards (Art. 42) and by the way of derogations (Art. 44). The current wording of these provisions only refers to situations where no adequacy decision has been taken, which makes their scope of application ambiguous.

It should be considered whether standard data protection clauses devised by a DPA and BCRs could be adopted under a procedure not as lengthy as the consistency mechanism. While we recognise the need for a coherent application of the data protection rules, we believe that subjecting cross-border data transfers to this multi-step process constitutes a serious obstacle to the free flow of data.
13. **Penalties for infringements of data protection rules have to be reduced**

EUROCHAMBRES deems the administrative sanctions for non-compliance with the draft Regulation disproportionately high, especially from an SME point of view. Moreover, as the sanctions are dependent on a company’s turnover, it is impossible to predict their actual amount. The Chamber network recommends that the penalties be reduced and capped, and should be independent of a company’s turnover. Also, DPAs should be allowed to send a warning letter instead of imposing a fine in all cases and not just in the two situations listed in the draft proposal.

The regulation makes it mandatory to impose fines. Serious and well-intentioned actors should not be treated the same as intentional or repeated offences. The mandatory approach also complicates the interactions between businesses and the supervisory authority. This may hinder innovation in new services and make it more difficult for SMEs.

14. **Additional transitional provisions are needed**

The draft Regulation lacks transitional provisions. In particular, EUROCHAMBRES has doubts whether consents for data processing collected before the draft Regulation’s entry into force would remain valid, given the new requirement for a data subject’s explicit consent (see point 6). If this requirement is retained in the Regulation, an additional provision would be necessary, stipulating that the consents gathered under the previous regime are still valid.

15. **No need to allow organisations to bundle claims (art. 73.2)**

Enforcement of data protection regulation is already in the hands of the data supervisory authority and we do not see the interest of introducing a mechanism of collective redress or group action in this peculiar context.