Recommendations on the Implementation of the General Data Protection Regulation

The European Data Coalition (Coalition) is committed to contribute to the development of a progressive data protection framework, where both clarity and consistency are ensured. In the context of the implementation of the General Data Protection Regulation (GDPR), the Coalition welcomes the ongoing culture of proactive and high-level engagement between all stakeholders including industry representatives, privacy professionals, the European Commission, the European Data Protection Supervisor (EDPS), the Article 29 Working Party (A29WP) and the EU Data Protection Authorities (DPAs).

The Coalition has emphasised the necessity of protecting the fundamental right to privacy and increasing trust in data processing activities, but we have also reminded stakeholders that privacy is not absolute and that it must be considered in relation to its function in society. The implementation and interpretation of the GDPR must create as much legal certainty as possible as well as preserving flexibility to support innovation in Europe. Consequently, any guidance issued by the EU DPAs and the Commission needs to be "future-proof" and technologically neutral.

The recommendations below are based on the Coalition's GDPR Manifesto and aim to strike a balance between the provisions laid down in the GDPR and the reality faced by European companies seeking to implement them, by providing advice on workable solutions to bring about effective context-specific compliance, drawn from real-life business experiences.

Data Processing and the Rights of the Data Subject

Lawfulness of data processing (Article 6)

The grounds for processing personal data under the GDPR broadly replicate those under the Data Protection Directive. However, the GDPR sets a more demanding framework of justifications for lawful processing, and adds a new principle of accountability.

More particularly, the GDPR raises the bar for valid consent much higher. Consent must be fully unbundled from other terms and conditions and will not be valid unless freely given, specific, informed and unambiguous [Arts 4(11) and 6(1)(a)]. The GDPR also narrows the legal justification allowing for data controllers to process in their legitimate interests. This justification also appears in the Directive, but the interpretation of the concept in the current regime can vary significantly among the different Member States, considering Art. 6(2).

Moreover, the justifications and conditions for processing special categories of data are areas in which where Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Challenge 1: If Member States are allowed to adopt specific national or local laws relating to the lawfulness of data processing, the concept of harmonization in data-based activities in the EU is undermined. For instance:

- There are new limitations on the use of consent and the processing of children's data. Notably, Member States are permitted under Art. 8(1) to vary the age trigger assigned to the provision on processing of children's personal data between 13-16 years old.
- According to Art. 6(2), Member States are allowed to introduce local and more specific rules on processing for the compliance of a legal obligation and for the performance of a task carried out in the public interest.
- Whistleblower systems have been around for many years now. Article 6.1 f) of the GDPR will be the legal basis for processing personal data in such systems. These are recognized as a legal means for assisting companies with legal compliance to the benefit of society at large. Legislation across the EU promotes the use of these systems, but the regulatory variations that still persist on the use of these tools creates challenging uncertainties for companies operating across the EU. Indeed, the necessary research on these variations and the subsequent adaptation to the different national requirements is costly for companies with an EU-wide presence. It is doubtful that the workforce, taking advantage of the right of free movement within the EU to change their country of employment, experience any benefit from these differences. Rather, it creates unnecessary costs at no actual benefit for data subjects.

Recommendation 1: Harmonization and consistent application of rules should be strongly supported. The 29WP, the national DPAs and the Member States should adopt a common approach on the application of rules on consent by children, on conditions to process data in compliance of a legal obligation and the performance of a task carried out in the public interest.

Considering the free movement of persons, it would be helpful for employees, just as it would be for international companies, if the rules would be harmonized and clear and national deviations avoided.

Challenge 2: Following Art. 6(4), there are specific restrictions on the ability to rely on legitimate interests as a basis for processing. There is a non-exhaustive list of factors to be taken into account when determining whether the processing of data for a new purpose is incompatible with the purposes for which the data were initially collected.

The level of subjectivity in the assessment of compatibility in further processing and the uncertainty as to who determines this creates difficulties to innovative technologies such as Big Data, Internet of Things, machine learning and artificial intelligence. A few examples:

- Data may have been processed in an IT-system to deliver a specific service [processing made under article 6.1 b)], yet through additional analytic data processing it is found that at certain times of the day the service is slow due to larger than average usage. The analytics can be used to develop a new function or service that evens out the usage so the ordinary speed of service can be upheld.

- The same situation as above except that the purpose of the analytics is to create statistics that can be used for improving the transportation network and reducing traffic jams, or for estimating future stock/inventory of goods.
- There is a suspected breach of an employer's internal rules and instructions, which may harm both individuals and/or the employer. The internal rules and instructions and the fact that personal data may be processed to investigate the breach is communicated. The first purpose for data processing is to fulfil work tasks and the additional processing is used to investigate the breach.
- Individual persons provide their personal ID details (name, address, phone number etc.) for registration in a loyalty program developed by a retail company. Those personal data are processed for the management of such a loyalty program and within the terms authorised by the data subject. The retail company (controller) may also use the personal data at a certain point of the loyalty program, for fraud control purposes – by checking if the data are, in any way, related to fraudulent acts regarding the loyalty card of the data subject. This is a new service provided by the controller under the loyalty program, which goes beyond its scope but is for the direct protection and benefit of the data subject and, as such, this secondary purpose should not be itself unlawful.

Recommendation 2: The fact that there is no connection between the initial purpose of collection and the new secondary purpose does not in itself make the purpose incompatible. It is recommended that guidelines are issued which clarify that personal data may be processed, *inter alia,* for the purpose of improving products and services and developing new products and services.

There are numerous ways analytics can be used. It may therefore be better to specify in guidelines what would be a prohibited new use. Moreover, if a company's privacy lead has done an Impact Assessment and determined that appropriate privacy mitigations are in place, there should be a presumption of lawfulness. The GDPR requires a high level of transparency (as to when legitimate interests are being used), so this is not a particularly risky proposition, nor one that can be challenged by those that disagree with the assessment.

Data portability (Article 20)

According to Art. 20, when controllers process personal data through automated means, data subjects will have the right to obtain a copy of their personal data from the controller in a commonly-used format and have it transferred to another controller. Where feasible, the controller may even be required to transmit the data directly to a competitor. However, Recital 68 limits this right, so that it applies only when processing was originally based on the user's consent or on a contract. It does not apply to processing based on a public interest or the controller's legitimate interest.

Challenge 3: It is not clear how the obligation would interact with other legal areas (e.g., intellectual property (such as database rights and trade secrets), competition, etc.) and with innovative markets (e.g., cloud computing, Internet of Things, data security). Art. 20 is also unclear as to the exact scope of the personal data to provide to the data subject, for instance, on what data should be ported. A few examples:

- Company A keeps an internal database about its business partners (Companies B-Z). The database includes names, business addresses and business phone numbers and other data

similar to what is normally stated on business cards. The database also includes data on subscriptions to newsletters (collected with consent or to fulfil a contract) and other details (collected with consent) relating to the business partners' employees. The database is subject to both database and trade secret protections. The data subject has the same data and can provide it itself to a competitor of Company A. There is no consumer interest for the data subject to have the data ported over to a competitor of Company A. Furthermore, there is no actual consumer interest in having any future releases of the database designed (under Privacy-by-Design principles) to include a new portability function. The portability requirement would therefore only drive costs without any legitimate benefit and would be contrary to the principles of fair competition which database and trade secret rights aim to protect.

- A company maintains a social media platform where employees can by their own choice post their profile with both professional skills, professional interests and personal interests. The platform is used as a collaboration tool for the company's business so the employees use it to exchange various types of information, questions and answers. The data posted includes copyright-protected works and trade secrets. One question with data portability which then arises is that of what personal data is in this context. Even if it is found to be strictly limited to personal interest there is no consumer interest that the personal data should be portable. The portability requirement would therefore only drive costs without any legitimate benefit.
- A company maintains a database with employee evaluations based on consent. The data is used for training employees and for professional growth and career orientation. The evaluations are part of the strategic plan for developing the business in a certain direction and not to be ported to competitors and others. It is closely connected to running a business and can also be part of the confidential information of the company.
- A company has a loyalty program for its clients, which aims to grant them special sales conditions. Under the management of this loyalty program, the company (controller) develops statistics information on products which are top sellers among the clients registered in this program, patterns of sales etc. This kind of information should be considered as a trade secret and, therefore, should not be transmitted to any other controller/competitor.

Recommendation 3: Guidelines should be produced on consistent and effective implementation, interpretation and enforcement of the obligation on data portability in relation to other legal areas and innovative markets. Rules should be interpreted to limit the right to data portability to data provided by the consenting data subject, but not all the (non-personal) data generated during lawful processing, which represents confidential information held by the company/processor, and should be treated as a trade secret. An excessively broad interpretation of this right could create obstacles to the protection of intellectual property rights, protected commercial information and data belonging to third parties.

- Scope: Clarify the scope of the right to data portability and in particular limit the portability requirement to abstain from obliging companies to disclose confidential business information and trade secrets (namely profile information), in order to guarantee that there will not be any further data transfer to a competitor.
- Non-relevant systems: Data portability should be clarified to be limited to certain types of private related activities where it is relevant and not when they concern information processed in the employment context or in other business activities. It should be clarified that the portability requirement applies when there is a clear consumer interest.

- Tech-neutrality: Guidelines emerging from either the EDPB or the Commission must avoid establishing technology 'winners' and 'losers,' by establishing a preference for specific file formats, technology approaches or means to achieve compliance.

Challenge 4: Portability is an improvement for certain types of consumer services but processing of data can occur where there is no compelling consumer interest. It imposes excessive financial burdens upon companies having to comply with the new obligation in order to avoid that innovation and competition are stifled.

Recommendation 4: Promote a balanced approach so that data portability is limited to data in private activities where it is motivated by a compelling consumer interest.

Profiling (Article 21)

Under Art. 21, individuals have a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them. However, such significant automated processing can be used if it is: i) necessary to enter into, or to perform, a contract between a data subject and controller; ii) authorised by Union or Member State law; or iii) based on the individual's explicit consent.

Challenge 5: Article 22(4) determines that profiling-based decisions shall not be based on special categories of personal data (e.g. racial, ethnic, or religious information) unless (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where prohibited by Union law or member state law; or (b) processing is necessary for reasons of substantial public interest, on the basis of Union or member state law. Even in these circumstances, described more fully in Article 9(2)(a) and (g), the controller must still ensure "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place."

Recommendation 5: the Commission, A29WP and Data Protection Supervisor should provide more guidance on the circumstances under which profiling-based decisions are permissible for special categories of personal data, according to Art. 22(4). It should also clarify what are the implications of Art. 22's vague expression "legal effects concerning him or her or similarly significantly affects him or her". For instance, could direct marketing including specific offers or discounts based on profiling fall under this definition?

Challenge 6: according to Art. 21(2) it is unclear whether a customer should have the right to receive marketing offers but reject any profiling connected to them, or whether all data subjects that consent to marketing can also be profiled in order to receive relevant and specific information and offers.

Recommendation 6: the A29WP should also ensure the production of harmonised guidelines regarding the definition of "legal effects concerning him or her or similarly significantly affects him or her" in Art. 22.

Processes and Formalities

Data Breach Notification (Articles 33.1, 34.1 and 71.h)

Data controllers must notify most data breaches to the DPA. This must be done without undue delay and, where feasible, within 72 hours of awareness. A reasoned justification must be provided if this timeframe is not met. In some cases, the data controller must also notify the affected data subjects without undue delay.

The DPA does not need to be notified if the breach is unlikely to present risks to the rights and freedoms of individuals.

Challenge 7: Without a clear definition of "risk" and "high risk", notification obligations look burdensome on data controllers, data subjects and DPAs. If the data breach needs to be reported within 72 hours, all necessary steps will be made under enormous time pressure and it may not always be possible to consult with the Data Protection Officer. Consequently, any uncertainty in definitions will only cause delays in the smooth reporting of data breaches.

Recommendation 7: See, below, Recommendation 1 in the section on Data Protection Impact Assessment (DPIA). Confirmation is needed on whether the concept of "high risk" as included in the provisions relating to data security breaches is to be understood in the same way as in the DPIA context. Risk related to sensitive data is characterized as "significant" (Recital 51). Clarification is needed on how "high risk" should be quantified in relation to "significant" risk.

Challenge 8: There is no clear definition of what may represent "likelihood to result in a risk to the rights and freedoms of natural persons". Indeed, such an understanding might differ among companies and processors, depending on their own activities and the sectors in which they operate. It is also unclear how and when the data breach should be notified to data subjects. A few examples:

- An IT company specialised in cybersecurity services has a natural predisposition to better ascertain whether certain conducts might have present potential risks to the rights and freedoms of their clients/data subjects; on the contrary, a Marketing Agency, with no know-how and internal expertise in IT related issues, will not have such predisposition and internal resources to carry out such an assessment.
- A company suffers an attack from a hacker to its clients' database; the hacker claims to have full access and control of all personal data stored, and demands a monetary settlement to cease his unlawful conduct and to prevent him from selling those data to a third party or to make use of them. There is not any evidence about the truth of such allegations from the hacker. According to the GDPR, in such situation the processor should notify, with no delay, the data subjects affected. However, such notification might be almost impossible to execute in due time and may even be harmful: a) firstly, it might be a false claim which will only unnecessarily alert the date subjects about the situation b) secondly, even if the claim is true, the execution of the notification might raise the media's attention, which could disturb the National DP Authority's and the Police's ongoing investigations; c) in practical terms, it might not be possible to notify all the data subjects affected in less than 2/3 days, especially if they belong to a huge database from a big company and thousands of clients have to be notified.

Recommendation 8: we recommend the following:

- List of hypothetic situations that are highly likely to represent a risk to the rights and freedoms of the natural persons and, as such, require a prompt notification of data breach to the Supervisory Authority.
- List of typical breach situations which must be reported to authorities and data subjects, to help companies to ensure legal compliance and at the same time not create un-called for concerns for data subjects.

Challenge 9: For communication service providers, the alignment of this notification procedure with the notification regime under Regulation 611/2013, which details a specific procedure for breach notification laid out in Article 4 of Directive 2002/58/EC ("e-privacy Directive") becomes somehow confusing, especially in light of the announced revision of the e-Privacy Directive. Indeed, Regulation 611/2013 applies to the notification of personal data breaches by providers of publicly available electronic communications services (e.g. telecommunication companies, ISPs and email providers). According to this Regulation, the provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible.

Further to this, on July 25, the EDPS issued a preliminary opinion (Opinion 5/2016) on the review of the e-Privacy Directive, in which it recommends deleting Articles 4.3 and 4.4 of the e-Privacy Directive on data breaches as the GDPR already requires all controllers to notify subscribers and competent national authorities of personal data breaches (subject to certain exemptions). To avoid duplication, the EDPS recommends that all data breaches involving personal data should be notified to the supervisory authorities provided for in the GDPR according to the provisions set forth therein.

Recommendation 9: in the forthcoming revision of the e-privacy Directive, both the Commission, the A29WP and the EDPS should articulate their work in order to avoid any changes to the Directive that may contradict both provisions from GDPR and Reg. 611/2013 on data breach notifications. There should be some guidance on the relation between these two regimes, by clarifying that for these providers, the notification requirements to be considered are those laid down in Regulation 611/2013. The Commission should consider the deletion of the articles concerning data breaches in the announced revision of the e-privacy Directive.

Data protection impact assessments (Article 35)

The GDPR places onerous accountability obligations on data controllers to demonstrate compliance. This includes requiring them to maintain certain documentation, conduct data protection impact assessments for more "risky processing activities" and implement data protection by design and default.

Challenge 10: Without a clear definition of "risk" and "high risk", accountability obligations appear to be burdensome on data controllers, data subjects and the DPAs.

Recommendation 10: Guidance on the definition of "risk" and "high risk" should be given, taking into account the following considerations:

- High risk: In Art. 35, clarification should be given on the implications and meaning of: i) "type of processing in particular using new technologies", ii) "nature, scope, context and purposes of the processing", iii) "is likely to result in", iv) "high risk to the rights and freedoms of natural persons".

    - Large-scale processing operations: Recital 91 confirms that these operations do not necessarily pose high-risks and sets out a number of other cumulative criteria. It states, for instance, that a DPIA should be made where personal data are processed for taking decisions based on "systematic and extensive" profiling of "specific" natural persons or profiling based on "the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures". Clarification is needed on the meaning of terms such as "systematic and extensive", as it can be argued that these are not the critical elements that necessarily result in "high risk".
    - Monitoring publicly accessible areas: Recital 91 mentions that a DPIA is required for "monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices". Clarification is needed on the scope of the terms "publicly accessible areas" and "large scale".
    - Any other operations: Recital 91 further adds that "any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale". The provision foresees, therefore, that a DPIA could be required for "any" operations where the competent authority, and not the organisation, considers that processing is likely to create a high risk. We recommend that this provision is interpreted narrowly and in alignment with Art. 35.

- The prior consultation process: It is unclear when the controller needs to consult the supervisory authority. If the DPIA indicates that the processing would be highly risky, as part of a DPIA the controller will seek to introduce appropriate measures to mitigate the risk. The language in Article 36 however requires that the controller should consult the supervisory authority if the DPIA indicates that "the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk". Clarification is needed concerning whether the processing can go ahead without an obligation for prior consultation in cases where the DPIA identifies a situation of high risk but the controller introduces measures that according to his assessment mitigate this risk.
- Risk: Recital 75 gives important guidance on how "risk" should be understood, but further clarifications are needed on the type of "objective assessment" that would be expected in order for organisations to establish whether data processing operations involve a "risk" or a "high risk".

Challenge 11: Data Protection Impact Assessments (DPIA) can be a tool which can help companies identify the most effective way to comply with their data protection obligations and meet data subjects' expectations of privacy. However, the practical implementation of these DPIA's raise many doubts and questions for companies and for their information security systems.

Recommendation 11: in order to mitigate some of the uncertainties, we recommend the following:

- Flexibility: production of non-obligatory templates or minimum elements to be included in each DPIA. Each organisation is best placed to determine the most effective methodology depending on the sector in which they operate, the type of data they process, the processing activities in which they are engaged, their existing internal policies and procedures;
- Simplicity: an excessively broad definition of "high risk" would lead to DPIAs being unnecessarily required. It is necessary to avoid such an overload and allow DPAs to ensure that meaningful and effective assessments are made.
- Clarity: indicative lists should be produced on "the kind of processing operations which are subject to the requirement for a data protection impact assessment" and on "the kind of processing operations for which no data protection impact assessment is required" (Art. 35/4 and 5).

Role of Authorities

Tasks of European Data Protection Board (Article 70)

An independent European Data Protection Board (EDPB) is to replace in 2018 the A29WP and will include the European Data Protection Supervisor (EDPS) and the representatives of the EU DPAs. Its obligations will include issuing opinions and guidance, and ensuring a consistent application of the GDPR. The EDPB will also play a role in the one-stop-shop-mechanism.

Challenge 12: Art. 70 creates the EDPB but it is unclear as to certain practicalities such as budget, scope of mandate and how its independence is to be guaranteed. A weaker EDPB would not be able to ensure the consistent application of the GDPR across the EU, nor would it be in position to promote harmonization on those elements in the GDPR that permit Member State discretion and deviation. Furthermore, if the independence of the EDPB is not guaranteed and supported by adequate financial means, the risk of it being captured and influenced by stronger individual DPAs increases.

Recommendation 12:

- Institutional design: The EDPB will replace the A29WP and aggregate the European Data Protection Supervisor (EDPS) and the national DPAs. A clear and transparent understanding of its role, as well as of its functions and accountability across its members should be ensured as early as possible. The functional relationship with the European Data Protection Supervisor and the European Commission should also be clarified.
- Independence: To avoid that the EDPB is captured by individual and strong DPAs, independence from national pressures and local interpretations must be accepted and enforced from the beginning. To safeguard its independence and the pursuit of the full scope of the its mandate in line with Recital 4, as well as the achievement of better regulation principles, a chief economist function should be created within the EDPB.
- Scope: the scope of competence of the EDPB is ambitious, from producing guidelines, to ensuring consistency and serving as a dispute resolution mechanism for disputes between regulators, notably between the "*lead* supervisory authority" and other "supervisory authorities." Future activities carried out by the EDPB should include:
    - Supervise the consistency with EU law and practice of any additional measures the GDPR allows the EU member states to adopt at national level;

- Develop procedures that facilitate a transparent and efficient interaction with businesses and consumer organisations, including the ability to request that matters are reviewed, particularly in light of new emerging technologies and societal benefits brought about by innovation;
- Reaffirm that all EDPB decisions under the GDPR fully consider all fundamental rights and EU objectives as stated in Recital 4.

- Resources: in order for the EDPB to operate efficiently and with independence, a transparent and adequate financing system must be ensured, from both the EU's and national budgets. (…)

Challenge 13: The EDPB is charged with providing recommendations on application of data protection law without the benefit of formal requirements for public consultation with all relevant stakeholders, nor with the benefit of the type of economic analysis routinely expected in the Commission context when major policy recommendations are put forward.

Recommendation 13: EDPB should guarantee, for each and every mandate, that the members are duly advised on issues related to Information Technology implied in personal data processing systems built up by companies. To safeguard the complete and accurate understanding of technical implications derived from the implementation of the GDPR, EDPB's members should be advised, at all time during their mandate, by trained and skilled experts with specific expertise in the fields of Innovation and Information Technology, with profound and proven knowledge and experience on areas such as cybersecurity, cloud computing, *Big Data*, risk management, among others.

Furthermore, appropriate EU-level funding must be secured for DPAs to promote independence and enhance the role and effectiveness of representatives from smaller or less-well-funded Member States. Also, mechanisms for public and/or stakeholder consultation by the EDPB should be institutionalized, to enhance the quality of the work product of the EDPB.

Sanctions and Liability

Right to Compensation and Liability (Article 82.3)

Under the GDPR, controllers and processors will be jointly liable for data protection violations. This means that the data subject is entitled to full compensation from any of the parties. Liability for damages subsequently may be apportioned among them according to their respective responsibility for the harm.

Challenge 14: There are no common standards for documentation for processors to ascertain compliance with GDPR rules.

Recommendation 14: The accepted standard for documentation for processors to prove their compliance with the GDPR needs to be clarified and harmonized on an EU-wide level. Such standards will help the processor to confirm that the processor has fulfilled the required controls. It will also ensure that the processor is not jointly and severely liable merely due to a lack of acceptable documentation;

Sanctions/Administrative fines (Article 83)

The GDPR establishes a tiered approach for penalties for breach, which enables DPAs to impose fines for some infringements (e.g., breach of requirements relating to international transfers or the basic principles for processing, such as consent) of up to 4% of the annual turnover or of 20 million euros – whichever is higher – in the case of undertakings. Other specific infringements would attract a fine of up to 2% of annual worldwide turnover or 10 million euros (again, whichever is higher).

The concept of undertaking is defined in the recitals of the GDPR in reference to Arts. 101 and 102 of the TFEU.

Challenge 15: fines are a necessary part of meaningful data protection regimes. An inconsistent interpretation on what are aggravating and mitigating circumstances assessed in the context of the imposition of sanctions, or on the meaning of what is a minor infringement, leads to different national practices and the fragmentation of the market. Uncertainties in the level of harmonization of sanctions and fines increases the risk and cost of doing business.

A regime that does not equally take into account the principles of proportionality and necessity creates fewer incentives for taking business risks in data driven innovations resulting in delayed time to market and loss of first mover advantage.

Recommendation 15: the A29WP and the Commission should work together in developing guidelines on the application of sanctions to be followed by the different DPAs. A common interpretation of the existing rules would ensure legal certainty and a level playing field for companies and consumers across the EU, who would be sure that all 28 national data protection authorities applied the same criteria for assessing a breach. A common understanding of the rules on sanctions should reflect the following considerations:

- Role of DPAs:
    - DPAs should follow a clear enforcement pyramid: 1) Information; 2) Persuasion; 3) Warning letter and 4) Civil sanctions.
    - DPAs should only have the right to engage in civil sanctions if serious harm is caused to the data subject or if the controller has disregarded previous warning letters, and provided that there is a serious risk for the individual. The mere breach of formalistic requirements without supporting evidence of damage to data subjects shall not lead to civil sanctions.
    - Only the lead authority shall have the power to issue penalties, consistently with an agreed one-stop-shop-model.
    - A successful enforcement strategy should focus on increased detection of data breaches by primarily fostering trust between the regulator and the regulated with a cautious use of punitive sanctions as a last resort.

- Proportional Fines:
    - Fines should be zero or minimal if the concerned organisation has taken serious steps to act responsibly and mitigate risks in its data processing activities. An example of a serious and responsible step might be the implementation of a corporate roadmap of compliance on data security developed by a company. A related example: the

roadmap of compliance identifies a specific kind of occurrence and covers IT measures to mitigate or delete it – however, due to external factors, and to the lack of time for complete implementation, this specific occurrence (which represents a real infringement of an obligation under GDPR) takes place only 2 days after the roadmap has started to be implemented.

- Funding Through Fines: DPAs may not finance their activities with fines accrued from civil sanctions. All proceeds from civil sanctions shall be used for certification institutes and other means to enhance privacy.

Certifications and Codes of Conduct

Code of Conduct (Article 57m)

The GDPR endorses the use of codes of conduct and certifications to provide guidance on the GDPR's requirements, as a signal to data subjects and regulators that an organization is in compliance with the Regulation, and offering third-party oversight as another check on companies' data handling practices.

Challenge 16: The efficient development of codes of conduct will rely heavily on frequent engagements between industry and the national DPAs. From the Commission's perspective, codes of conduct should be developed by Industry.

Recommendation 16: the development and approval process of codes of conduct should be flexible, Industry-led and following a multi-stakeholder approach. Further considerations:

- DPAs & EC's involvement: the scrutiny of DPAs and the Commission in endorsing codes of conduct would increase its value. In addition, such codes should have a European scope and the EC should serve as a facilitator. DPAs should be involved in monitoring compliance with codes of conduct.
- Incentivizing the development and adoption of codes of conduct: the promotion of codes of conduct among businesses could be significantly improved through the use of unified tools (i.e., standardized operational procedures, including business process software) and we encourage the support of the concerned authorities, including the Commission, to assist in speeding up the EU-wide applicability of such tools.
- Industry's role: codes of conduct should be preceded by industry-led negotiations following a multi-stakeholder approach. For Industry, the added value would be to demonstrate commitment to high compliance standards and to create trust in the system.

Employment Data

Processing in the employment context (Article 88)

Member states have the right to provide their own specific rules. But in order not to lose the benefit of the harmonization provided by the regulation, Member States' proposals concerning the processing of employee data should be monitored.

Challenge 17: The GDPR expressly authorizes individual Member States to implement more specific rules in respect of the processing of HR-related data. This means that specific rules regarding the

processing of personal data for the purpose of recruitment, the performance of the employment contract, diversity, health and safety can be adopted differently on a national level. This level of discretion frustrates the objective of harmonization, reduces legal certainty and increases the costs for companies operating in more than one Member State. Examples of where Member State legislation is needed:

A29WP has called into question whether consent is ever an appropriate legal basis for data processing in the HR context due to the inherent imbalance in the employee-employer relationship, but alternate bases are often restricted.

Recommendation 17: in order to address the risk of fragmentation and the increase in cost for companies operating in more than one Member State, we recommend the following:

- A29WP to issue guidelines and promote the advantages of a consistent application of rules;
- Commission to clarify the expectation that affirmative enabling legislation be put forward by Member States to support common HR-use cases, particularly in the areas of health-benefits processing, background screening implicating criminal history.
- A29WP to clarify that "in furtherance of an employment contract" is indeed a legitimate basis for processing large classes of personal data in the HR context.

Challenge 18: A29WP has called into question whether consent is ever an appropriate legal basis for data processing in the HR context due to the inherent imbalance in the employee-employer relationship, but alternate bases are often restricted.

Recommendation 18: A29WP to clarify that "in furtherance of an employment contract" is indeed a legitimate basis for processing of large classes of personal data in the HR context.

Consistent Application

Derogations and Special Conditions

The GDPR contains several derogations and exemptions regarding the restrictions to obligations, data protection rights and certain specific processing situations. This is likely to result in a harmful degree of variation across the EU, demanding from European companies operating across the EU a permanent adjustment to different approaches adopted nationally by the Member States.

Challenge 19: In the text of the GDPR there are approximately 30 instances in which Member States have been given the ability to legislate at a national level. These are the key provisions in the GDPR which contain possibilities for national law derogations:

- Legal grounds for processing – Arts. 6/2, 9/2(a) and 9/4
- Children data – Art. 8
- Fines and sanctions – Arts. 58/6, 84/2
- Data subject rights limitations – Art. 23/1
- International data transfers – Art. 49/5
- Requirements for specific processing situations (e.g., employment data) - Arts. 85-91

This will result in national law differences in Member States and businesses will still need to consider data protection laws in different parts of the EU. While some national Supervisory Authorities might take a strict approach limiting the scope of action for businesses, others might be more commercial in

their approach and implement derogations which can assist businesses in their compliance with the GDPR.

Recommendation 19: As mentioned earlier, this level of discretion frustrates the objective of harmonization, reduces legal certainty and increases the costs for companies operating in more than one Member State. A29WP and the European Commission need to ensure a consistent application of the new rules as early as possible.

Challenge 20: A company is established in a certain Member State but also carries out activities in one or a few of its neighbouring Member State(s), but the managing team responsible for the control of all information systems storing and securing all the data processed (both domestically and abroad) is the same. If the National Supervisory Authorities of both countries have different approaches in relation to some of the provisions of the GDPR, this company will face increased costs for adapting each of the requirements of National Supervisory Authorities applicable to each Member State and the legal harmonization (which is one of the main drivers of this GDPR) is completely frustrated.

Recommendation 20: the EC, the EDPB and the national Supervisory Authorities should cooperate closely, and have a coordinated approach between them to advise National Governments and Parliaments, and to issue some guidance in order to promote the greatest level of consistency and avoid the unnecessary costs of further fragmentation across EU.

ABOUT THE COALITION

Our Coalition is made up of twenty-one European companies, from SMEs to Global Multinationals and non-profit organisations operating in a variety of sectors on a national, regional and global scale. With an aggregate turnover (2015) of over € 222 billion and some 968,000 employees worldwide, our footprint allows us to bring growth, progress and jobs to the EU's economy. Our membership includes…

… a global leader in power and automation solutions…
… the leading Central and Eastern European e-commerce company…
… a productivity solutions provider of compressors, vacuum solutions, construction and mining equipment…
… a non-profit organisation dedicated to collecting money to prevent and combat child cancer diseases…
… a global leader in household appliances…
… two providers of communications technology and services…
… a designer, engineer, manufacturer and distributor of outdoor power products…
… a multinational retail-clothing company…
… an investment company…
… a SME provider of online marketing through search engine marketing, conversion and lead generation…
… an e-commerce company providing payment services for online storefronts…
… an engineering group in tooling, materials technology, mining and construction …
… an enterprise software corporation…
… a global provider of heavy trucks and buses, engines and services…
… a global provider of renewable solutions in packaging, biomaterials, wood and paper…
… a multinational company managing a portfolio of businesses in retail, financial services and technology…
… the leading university in technology and digital arts programmes…
… a provider of business software and services to more than 340 000 business in the Nordics…
… a producer and distributor of trucks, buses and construction equipment…
… the leading company in advanced mobile services…

Our businesses are profoundly different but deeply united by the need for clear, predictable and practical provisions, open cross-border data flows, balanced codified sanction guidelines, effective one-stop-shop and absence of overly prescriptive rules as fundamental conditions for long-term growth, competitiveness and prosperity, for both us and the economies in which we operate.

For further information please visit us www.europeandatacoalition.eu or contact us at frederico@europeandatacoalition.eu or rene@europeandatacoalition.eu