

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 3/2015 (with addendum)

Europe's big opportunity

EDPS recommendations on the EU's options for data protection reform



27 July 2015 (updated with addendum, 9 October 2015)

On 24 June 2015, the three main institutions of the EU, European Parliament, the Council and the European Commission entered co-decision negotiations on the proposed General Data Protection Regulation (GDPR), a procedure known as an informal 'trilogue'.¹ The basis for the trilogue is the Commission's proposal of January 2012, the Parliament legislative resolution of 12 March 2014 and the General Approach of the Council adopted on 15 June 2015.² The three institutions are committed to dealing with the GDPR as part of the wider data protection reform package which includes the proposed directive for police and judicial activities. The process should conclude at the end of 2015 and likely allow for formal adoption of both instruments in early 2016, to be followed by a two-year transitional period.³

The European Data Protection Supervisor (EDPS) is an independent institution of the EU. The Supervisor is not part of the trilogue, but is responsible under Article 41.2 of Regulation 45/2001 'With respect to the processing of personal data... for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '...for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. The Supervisor and Assistant Supervisor were appointed in December 2014 with the specific remit of being more constructive and proactive, and they published in March 2015 a five-year strategy setting out how they intended to implement this remit, and to be accountable for doing so.⁴

This Opinion is the first milestone in the EDPS strategy. Building on discussions with the EU institutions, Member States, civil society, industry and other stakeholders, our advice aims to assist the participants in the trilogue in reaching the right consensus on time. It addresses the GDPR in two parts:

- the EDPS vision for future-oriented rules on data protection, with illustrative examples of our recommendations; and*
- an annex ('Annex to Opinion 3/2015: Comparative table of GDPR texts with EDPS recommendation') with a four-column table for comparing, article-by-article, the text of the GDPR as adopted respectively by Commission, Parliament and Council, alongside the EDPS recommendation.*

The Opinion, published originally on our website and via a mobile app on 27 July, has been updated to include recommendations for the recitals to the GDPR. It will be supplemented in autumn 2015 with recommendations on the directive on data protection applying to police and judicial activities, once the Council has adopted its General Position on that directive.

The EDPS's comprehensive Opinion on the Commission's proposed reform package in March 2012 remains valid. Three years on, however, we needed to update our advice to engage more directly with the positions of the co-legislators, and to offer specific recommendations.⁵ As with the 2012 Opinion, this Opinion is in line with the opinions and statements of the Article 29 Working Party, including the 'Appendix' on 'Core topics in the view of trilogue' adopted on 17 June, to which the EDPS contributed as a full member of the Working Party.⁶

A rare opportunity: Why this reform is so important

The EU is in the last mile of a marathon effort to reform its rules on personal information. The General Data Protection Regulation will potentially affect, for decades to come, all individuals in the EU, all organisations in the EU who process personal data and organisations outside the EU who process personal data on individuals in the EU.⁷ The time is now to safeguard individuals' fundamental rights and freedoms in the data-driven society of the future.

Effective data protection empowers the individual and galvanises responsible businesses and public authorities. Laws in this area are complex and technical, requiring expert advice, in particular that of independent data protection authorities who understand the challenges of compliance. The GDPR is likely to be one of the longest in the Union's statute book, so now the EU must aim to be selective, focus on the provisions which are really necessary and avoid detail which as an unintended consequence might unduly interfere with future technologies. The texts of each of the institutions preach clarity and intelligibility in personal data processing: so the GDPR must practice what it preaches, by being as concise and easy to understand as possible.

It is for the Parliament and the Council as co-legislators to determine the final legal text, facilitated by the Commission, as initiator of legislation and guardian of the Treaties. The EDPS is not part of the 'trilogue' negotiations, but we are legally competent to offer advice, and to do so proactively in line with the Supervisor and Assistant Supervisor's remit on appointment, and the EDPS recent strategy. This Opinion leverages over a decade of experience in supervision of data protection compliance and policy advice to help guide the institutions towards an outcome which will serve the interests of the individual.

Legislation is the art of the possible. The options on the table, in the form of the respective texts preferred by the Commission, Parliament and Council, each contain many worthy provisions, but each can be improved. The outcome will not be perfect in our view, but we intend to support the institutions in achieving the best possible outcome. That is why our recommendations stay within the boundaries of the three texts. We are driven by three abiding concerns:

- a better deal for citizens,
- rules which will work in practice,
- rules which will last a generation.

This Opinion is an exercise in transparency and accountability, dual principles which are perhaps the most remarkable innovation of the GDPR. The trilogue process is coming under more scrutiny than ever before. Our recommendations are public, and we would urge all EU institutions to seize the initiative and to lead by example, so that this legislative reform is the outcome of a transparent process and not a secret compromise.

The EU needs a new deal on data protection, a fresh chapter. The rest of the world is watching closely. The quality of the new law and how it interacts with global legal systems and trends is paramount. With this Opinion the EDPS signals its willingness and availability to help ensure the EU makes the most of this historic opportunity.

TABLE OF CONTENTS

1	A BETTER DEAL FOR CITIZENS	5
1.1.	Definitions: let's be clear on what personal information is	5
1.2.	All data processing must be <i>both</i> lawful <i>and</i> justified	5
1.3.	More independent, more authoritative supervision.....	6
2	RULES WHICH WILL WORK IN PRACTICE	6
2.1.	Effective safeguards, not procedures.....	6
2.2.	A better equilibrium between public interest and personal data protection	7
2.3.	Trusting and empowering supervisory authorities	7
3	RULES WHICH WILL LAST A GENERATION	7
3.1.	Accountable business practices and innovative engineering.....	8
3.2.	Empowered individuals.....	8
3.3.	Future-proofed rules	8
4	UNFINISHED BUSINESS	8
5	A DEFINING MOMENT FOR DIGITAL RIGHTS IN EUROPE AND BEYOND	9
	ADDENDUM	10
	NOTES	11

1. A better deal for citizens

EU rules have always sought to facilitate data flows, both within the EU and with its trading partners, yet with an overriding concern for the rights and freedoms of the individual. The internet has enabled an unprecedented degree of connectivity, self-expression and scope for delivering value to businesses and consumers. Nevertheless, privacy matters more than ever to Europeans. According to the Data Protection Eurobarometer survey in June 2015,⁸ more than six out of ten citizens do not trust online businesses and two-thirds are concerned at not having complete control over the information they provide online.

The reformed framework needs to maintain and, where possible, raise standards for the individual. The data protection reform package was proposed firstly as a vehicle for ‘strengthening online privacy rights’ by ensuring people were ‘better informed about their rights and in more control of their information.’⁹ Representatives of civil society organisations wrote to the European Commission in April 2015 to urge the institutions to remain true to these intentions.¹⁰

Existing principles set down in the Charter, primary law of the EU, should be applied consistently, dynamically and innovatively so that they are effective for the citizen in practice. The reform needs to be comprehensive, hence the commitment to a package, but as data processing is likely to fall under separate legal instruments there must be clarity as to their precise scope and how they work together, with no loopholes for compromising on safeguards.¹¹

For the EDPS, the starting point is the dignity of the individual which transcends questions of mere legal compliance.¹² Our recommendations are based on an assessment of each article of the GDPR, individually and cumulatively, according to whether it will strengthen the position of the individual compared to the current framework. The point of reference is the principles at the core of data protection, that is, Article 8 of the Charter of Fundamental Rights.¹³

1.1. Definitions: let’s be clear on what personal information is

- Individuals should be able to exercise more effectively their rights with regard to any information which is able to identify or single them out, even if the information is considered ‘pseudonymised’.¹⁴

1.2. All data processing must be both lawful and justified

- The requirements for all data processing to be limited to specific purposes and on a legal basis are cumulative, not alternatives. We recommend avoiding any conflation and thereby weakening of these principles. Instead, the EU should preserve, simplify and operationalise the established notion that personal data should only be used in ways compatible with the original purposes for collection.¹⁵
- Consent is one possible legal basis for processing, but we need to prevent coercive tick boxes where there is no meaningful choice for the individual and where there is no need for data to be processed at all. We recommend enabling people to give broad or narrow consent, to clinical research for example, which is respected and which can be withdrawn.¹⁶

- The EDPS supports sound, innovative solutions for international transfers of personal information which facilitate data exchanges and respect data protection and supervision principles. We strongly advise against permitting transfers on the basis of legitimate interests of the controller because of the insufficient protection for individual, nor should the EU open the door for direct access by third country authorities to data located in the EU. Any request for transfer issued by authorities in a third country should only be recognised where it respects the norms established in Mutual Legal Assistance Treaties, international agreements or other legal channels for international cooperation.¹⁷

1.3. More independent, more authoritative supervision

- The EU's data protection authorities should be ready to exercise their roles the moment the GDPR enters into force, with the European Data Protection Board fully operational as soon as the Regulation becomes applicable.¹⁸
- Authorities should be able to hear and to investigate complaints and claims brought by data subjects or bodies, organisations and associations.
- Individual rights enforcement requires an effective system of liability and compensation for damage caused by the unlawful data processing. Given the clear obstacles to obtaining redress in practice, individuals should be able to be represented by bodies, organisations and associations in legal proceedings.¹⁹

2. Rules which will work in practice

Safeguards should not be confused with formalities. Excessive detail or attempts at micromanagement of business processes risks becoming outdated in the future. Here we may take a leaf from the EU's competition manual, where a relatively limited body of secondary legislation is rigorously enforced and encourages a culture of accountability and awareness among undertakings.²⁰

Each of the three texts demands greater clarity and simplicity from those responsible for processing personal information.²¹ Equally, technical obligations must also be concise and easily-understood if they are to be implemented properly by controllers.²²

Existing procedures are not sacrosanct: our recommendations aim to identify ways of de-bureaucratising, minimising the prescriptions for documentation and irrelevant formalities. We recommend legislating only where genuinely necessary. This provides room for manoeuvre whether for companies, public authorities or data protection authorities: a space that must be filled by accountability and guidance from data protection authorities. Overall, our recommendations would produce a GDPR text almost 30% shorter than the average length of the three institutions.²³

2.1. Effective safeguards, not procedures

- Documentation should be a means not an end to compliance; the reform must focus on results. We recommend a scalable approach which reduces documentation obligations on controllers into single policy on how it will comply with the regulation taking into account the risks, with compliance

demonstrated transparently, whether for transfers, contracts with processors or breach notifications.²⁴

- On the basis of explicit risk assessment criteria, and following our experience of supervising the EU institutions, we recommend requiring notification of data breaches to the supervisory authority and data protection impact assessments only where the rights and freedoms of data subjects are at risk.²⁵
- Industry initiatives, whether through Binding Corporate Rules or privacy seals, should be actively encouraged.²⁶

2.2. A better equilibrium between public interest and personal data protection

- Data protection rules should not hamper historical, statistical and scientific research which is genuinely in the public interest. Those responsible must make the necessary arrangements to prevent personal information being used against the interest of the individual, paying particular attention to the rules governing sensitive information concerning health, for example.²⁷
- Researchers and archivists should be able to store data for as long as needed subject to these safeguards.²⁸

2.3. Trusting and empowering supervisory authorities

- We recommend allowing supervisory authorities to issue guidance to data controllers and to develop their own internal rules of procedure in the spirit of a simplified, easier application of the GDPR by one single supervisory authority (the ‘One Stop Shop’) close to the citizen (‘proximity’).²⁹
- Authorities should be able to determine effective, proportionate and dissuasive remedial and administrative sanctions on the basis of all relevant circumstances.³⁰

3. Rules which will last a generation

The main pillar of the current framework, Directive 95/46/EC, has been a model for further legislation on data processing in the EU and around the world, and even provided the basis for wording of the right to protection of personal data in Article 8 of the Charter of Fundamental Rights. This reform will shape data processing for a generation which has no memory of living without the internet. The EU must therefore fully understand the implications of this act for individuals, and its sustainability in the face of technological development.

Recent years have seen an exponential increase in the generation, collection, analysis and exchange of personal information, the result of technological innovations like the internet of things, cloud computing, big data and open data, whose exploitation the EU considers essential to its competitiveness.³¹ Judging by the longevity of Directive 95/46/EC, it is reasonable to expect a similar timeframe before the next major revision of data protection rules, perhaps not until the late 2030s. Long before this time, data-driven technologies can be expected to have converged with artificial intelligence, natural language processing and biometric systems, empowering applications with machine-learning ability for advanced intelligence.

These technologies are challenging the principles of data protection. A future-oriented reform must therefore be predicated on the dignity of the individual and informed by ethics. It must redress the imbalance between innovation in the protection of personal data and its exploitation, making safeguards effective in our digitised society.

3.1. Accountable business practices and innovative engineering

- The reform should reverse the recent trend towards secret tracking and decision making on the basis of profiles hidden from the individual. The problem is not targeted advertising or the practice of profiling, but rather the lack of meaningful information about the algorithmic logic which develops these profiles and has an effect on the data subject.³² We recommend fuller transparency from controllers.
- We strongly support the introduction of the principles of data protection by design and by default as a means of kickstarting market-driven solutions in the digital economy. We recommend simpler wording for requiring the rights and interests of the individual to be integrated in product development and default settings.³³

3.2. Empowered individuals

- Data portability is the gateway in the digital environment to the user control which individuals are now realising they lack. We recommend allowing a direct transfer of data from one controller to another on the data subject's request and entitling data subjects to receive a copy of the data which they themselves can transfer to another controller.³⁴

3.3. Future-proofed rules

- We recommend avoiding language and practices that are likely to become outdated or disputable.³⁵

4. Unfinished business

The adoption of a future-oriented EU data reform package will be an impressive but nonetheless incomplete achievement.

All institutions agree that the principles of the GDPR should apply consistently to EU institutions. We have advocated legal certainty and uniformity of the legal framework, while accepting the uniqueness of the EU public sector and the need to avoid any weakening of the current level of obligations (as well the need to provide for the legal and organisational basis for the EDPS). A proposal consistent with the GDPR for the revision of Regulation 45/2001 should therefore be made by the Commission as soon as possible after the talks on the GDPR are finalised so that both texts can become applicable at the same time.³⁶

Secondly, it is clear that the Directive 2002/58/EC (the 'ePrivacy Directive') will have to be amended. Much more importantly, the EU requires a clear framework for the confidentiality of communications, an integral element of the right to privacy, which governs all services enabling communications, not only providers of publicly available electronic communications. This must be done by means of a legally-

certain and harmonising regulation which provides for at least the same standards of protection under the ePrivacy Directive in a level-playing field.

This Opinion therefore recommends calling for a commitment to speedy adoption of proposals in these two areas as soon as possible.

5. A defining moment for digital rights in Europe and beyond

For the first time in a generation the EU has an opportunity to modernise and to harmonise the rules on how personal information is handled. Privacy and data protection are not in competition with economic growth and international trade, nor with great services and products - they are part of the quality and value proposition. As the European Council recognises, trust is a necessary precondition for innovative products and services that rely on the processing of personal data.

The EU in 1995 was a trailblazer for data protection. Now over 100 countries across the world have data protection laws and less than half of these are European countries.³⁷ The EU nevertheless continues to command the close attention of countries who are considering establishing or revising their legal frameworks. At a time when people's trust in companies and governments has been shaken by revelations of mass surveillance and data breaches, this confers considerable responsibility on EU lawmakers whose decisions this year can be expected to have an impact not beyond Europe.

In the view of the EDPS, the GDPR texts are on the right track, but concerns remain, some very serious. There is always a risk with the co-decision process that certain provisions are weakened by well-intentioned negotiators in the search for political compromise. With data protection reform, however, it is different, because we are dealing with fundamental rights and the way they will be safeguarded for a generation.

On that basis, this Opinion seeks to assist the main institutions of the EU in solving problems. We want not just stronger rights for the individual data subject and greater accountability for the controller; we want to facilitate innovation with a legal framework that is neutral towards the technology but positive towards the benefits the technology can bring to society.

With negotiations in the final mile, we hope that our recommendations will help the EU get over the finishing line with a reform which will remain fit for purpose over the years and decades to come: a new chapter for data protection with a global perspective, with the EU leading by example.

Brussels, 27 July 2015

Giovanni BUTTARELLI
European Data Protection Supervisor

Addendum

On 27 July 2015 we published (EDPS Opinion 3/2015) our drafting recommendations for the operational clauses of the GDPR. Having now reflected on the underlying rationale behind the articles in the three versions advocated respectively by the Commission, European Parliament and Council, we wish to offer, as a further contribution to the ongoing trilogue negotiations, our recommendations on the content of the recitals to the GDPR.

The recitals in the preamble to an EU legal instrument are important because they explain the reasons for each provision. Though they have no independent legal value, recitals can be used when interpreting the scope of the substantive provisions in the text. The CJEU has stated on several occasions that valid recitals are necessary for the court to perform its function of interpreting the law. In providing the underlying rationale to the legal act, they merit careful consideration.

Accordingly, in these recommendations, we reiterate that respect for human dignity should be affirmed as the basis for all processing of personal information. The GDPR needs to be a blueprint for an ethical approach which embraces the societal benefits of technological change and innovation while shielding individuals from harm and empowering them to take control over the information about them in cyberspace. The recitals should provide greater incentive for accountability from controllers and room for guidance by supervisory authorities within the European Data Protection Board.

We continue to advocate drafting which is as clear, concise and intelligible as possible. Our recommendations would also remove from the recitals all unnecessary details which could limit flexibility to adapt to future challenges in an era where rapid change is the new norm.

Brussels, 9 October 2015

(signed)

Giovanni BUTTARELLI
European Data Protection Supervisor

Notes

¹ Joint Declarations European Parliament Council Commission Joint Declaration on Practical Arrangements for the Codecision Procedure (Article 251 of the EC Treaty) (2007/C 145/02), OJ C 145, 30.6.2007.

² COM(2012)11 final; European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), P7_TA(2014)0212; Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach, Council document 9565/15, 11.06.2015.

³ Long title is Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012)10 final; European Parliament legislative resolution of 12 March 2014 on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, P7_TA(2014)0219. On the timing and scope of the trilogue, see European Council Conclusions 25-26 June 2015, EUCO 22/15; a 'road map' for the trilogue was indicated at a joint Parliament-Council-Commission press conference <http://audiovisual.europarl.europa.eu/AssetDetail.aspx?id=690e8d8d-682d-4755-bfb6-a4c100eda4ed> [last accessed 20.7.2015] but has not been published officially. The GDPR will enter into force 20 days after its publication in the Official Journal and is expected to be fully applicable two years after its entry into force (Article 91).

⁴ Vacancy notice for the European Data Protection Supervisor COM/2014/10354 (2014/C 163 A/02), OJ C 163 A/6 28.5.2014. The EDPS Strategy 2015-2019 promised to 'seek workable solutions that avoid red tape, remain flexible for technological innovation and cross-border data flows and enable individuals to enforce their rights more effectively on- and offline'; Leading by example: The EDPS Strategy 2015-2019, March 2015.

⁵ EDPS Opinion on the data protection reform package, 7.3.2015.

⁶ See annex to Letter from Article 29 Working Party to V ra Jourová, Commissioner for Justice, Consumers and Gender Equality, 17.6.2015.

⁷ The material and territorial scope of the GDPR is difficult to summarise succinctly. The institutions seem to agree, at least, that the scope covers organisations established in the EU which are responsible for processing personal data either in the EU or outside it, organisations established outside the EU who process personal data of individuals in the EU in the course of offering goods or services to or monitoring individuals in the EU. (See Article 2 on material scope and Article 3 on territorial scope).

⁸ Other results included seven out of ten being concerned about their information being used for a different purpose from the one it was collected for, one in seven saying they their explicit approval should be required in all cases before their data is collected and processed, and two-thirds thinking it important to be able to transfer personal information from an old service provider to a new one; Special Eurobarometer 431 on data protection, June 2015. Comparable results from Pew Research in 2014 which found 91% Americans feel they have lost control over how companies collect and use person info, of social network users 80% are concerned about third parties like advertisers or businesses getting their data and 64% say government should do more to regulate advertisers; Pew Research Privacy Panel Survel, January 2014.

⁹ Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses.

¹⁰ Letter from NGOs to President Juncker, 21.4.2015 https://edri.org/files/DP_letter_Juncker_20150421.pdf and response from Head of Cabinet of Vice President Timmermans, 17.7.2015 https://edri.org/files/eudatap/Re_EC_EDRi-GDPR.pdf [accessed 23.7.2015]. The EDPS met with representatives of several of these NGOs to discuss their concerns on May 2015; PRESS RELEASE EDPS/2015/04, 1.6.2015, EU Data Protection Reform: the EDPS meets international civil liberties groups; full length recording of discussion available on EDPS website (https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Pressnews/Videos/GDPR_civil_soc).

¹¹ Article 2.2 (e).

¹² Article 1.

¹³ Article 8 of the Charter reads [emphasis added]

1. *Everyone has the right to the protection of personal data concerning him or her.*
2. *Such data must be **processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.** Everyone has the right of access to data which has been collected concerning him or her, and the **right to have it rectified.***
3. *Compliance with these rules shall be subject to **control by an independent authority.***

¹⁴ Article 10. Unless and until there exists a clear and legally-binding definition for 'pseudonymised data' as distinct from 'personal data', this type of data must remain within the scope of data protection rules.

¹⁵ Articles 6.2 and 6.4. Given that there has been some uncertainty as to the meaning of 'compatibility' we recommend, following the WP29 Opinion on Purpose Limitation, general criteria for assessing whether processing is compatible (see Article 5.2).

¹⁶ Effective functional separation is one means of ensuring lawful processing in the absence of consent, but legitimate interest should not be interpreted excessively. An unconditional right to opt out may also be an appropriate alternative in some situations. Assessing whether consent is freely given depends in part on (a) whether there is a significant imbalance between the data subject and the controller and (b) in cases of processing under Article 6.1(b), whether the execution of a contract or the provision of a service is made conditional on the consent to the processing of data that is not necessary for these purposes. (See Article 7.4.) This mirrors the provision in EU consumer law: under Article 3.1 of the Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer, 'A contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer'.

¹⁷ Such rules include adequacy decisions for specified sectors and territories, periodic reviews of adequacy decisions and Binding Corporate Rules. See Articles 40-45.

¹⁸ Article 73.

¹⁹ Article 76. On difficulty in obtaining redress for violations of data protection rules, see Fundamental Rights Agency report, Access to data protection remedies in EU Member States, 2013.

²⁰ EU rules place the emphasis on companies' self-assessment regarding compliance with TFEU Article 101 prohibition on anti-competitive agreements, while dominant firms in a market have a 'special responsibility' to avoid any action which might impair effective competition (Paragraph 9 of Commission Guidance 2009/C 45/02); see EDPS Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data, 14.3.2014.

²¹ The three texts refer variously to ‘intelligible manner and form, using clear and plain language’ (Recital (57), EP; Article 19, COM and Council), being ‘clear and unambiguous’ (Recital (99), EP; Article 10a EP) and providing ‘clear and easily understandable information’ (Article 10 EP, Article 11 EP), and information which is ‘concise, transparent, clear and easily accessible’ (Recital (25), EP, COM and Council; Article 11 EP).

²² Provisions for delegated acts have been largely removed in the versions of the Parliament and the Council. We believe the EU could go further and leave these technical matters to the expertise of independent authorities.

²³ Our recommendations would produce a text of around 20 000 words; the average length of the texts of the three institutions is around 28 000 words.

²⁴ Article 22.

²⁵ Articles 31 and 33.

²⁶ Article 39.

²⁷ Article 83. Research and archiving in themselves do not constitute a legal basis for processing, which is why we recommending deleting Article 6.2.

²⁸ Article 83a.

²⁹ The WP29 has outlined a vision for governance, the consistency mechanism and the one-stop-shop based on trust in independent DPAs and formulated in three layers:

- the individual DPA which is strong and fully resourced for dealing with cases within their sphere of competence;
- effective cooperation between DPA with a clear lead in cross border cases;
- the EDPB which must be autonomous, with its own legal personality, provided with sufficient means, consisting of equal DPAs working in a spirit of solidarity, with the power to make binding decisions and supported by a secretariat which serves the board through the chair.

³⁰ We also recommend clarifying the competence of the supervisory authorities and the designation of a lead authority in cases of transnational processing, whilst preserving the ability of the supervisory authorities to handle purely local cases. We recommend a simplified version of the consistency mechanism with more clarity on how to identify the cases where the supervisory authorities would need to consult the European Data Protection Board and where the Board would need to issue a binding decision in order to ensure the consistent application of the Regulation.

³¹ Commission Communication on A Digital Single Market Strategy for Europe, COM(2015) 192 final; European Council Conclusions June 2015, EUCO 22/15; Council Conclusions on the Digital Transformation of European Industry, 8993/15.

³² Article 14(h).

³³ Article 23.

³⁴ Article 18. We further recommend that, in order to be effective, the right to data portability must have a wide scope of application, and not only be applied to the processing operations that use data provided by the data subject.

³⁵ We recommend, for example, omitting terms like ‘online’, ‘in writing’ and ‘the information society’.

³⁶ One option, which we would prefer, is for this to be done by means of a provision in the GDPR itself.

³⁷ Greenleaf, Graham, Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority (January 30, 2015); (2015) 133 Privacy Laws & Business International Report, February 2015; UNSW Law Research Paper No. 2015-21.