AMENDMENTS TO THE DRAFT DATA PROTECTION REGULATION
PROPOSED BY BITS OF FREEDOM

On 25 January 2012, the European Commission published a proposal to reform the European data protection legal regime. One aspect of its proposal, a proposal for a new Regulation ("the Regulation"), aims to modernise and further harmonise the data protection regime created by the Data Protection Directive (95/46/EC).

Bits of Freedom believes that the Regulation on the whole is a step towards making data protection law fit for the 21st century. We welcome the fact that it starts from the standards and principles set out in the current Directive (95/46/EC) and further enhances, elaborates and improves a number of these standards and principles. Such improvements are necessary, as numerous incidents in recent years have clearly demonstrated that the privacy of internet users is regularly infringed. Both companies and governments have failed to handle data of citizens in accordance with data protection laws and principles. This has resulted in data breaches, circumvention of privacy rules, extensive and often furtive profiling of internet users and, increasingly, surveillance of citizens via social media and other channels.

To solve these issues, strong privacy standards are a must. The Regulation must effectively ensure the right of individuals to assert proper control over their personal data. In order achieve this, it is crucial to remedy a number of weaknesses in the Regulation that have the potential to undermine this right. Bits of Freedom calls for strong data protection rules that protect citizens in the online environment and that recognize the specific dangers associated with extensive tracking and profiling in the online environment. The first part of this document summarizes our key messages. The second part proposes amendments to specific articles.

I KEY MESSAGES

Our key messages, reflected in our amendments, are:

(1) **Properly define personal data**. The definition (and accompanying recital) of data subject (and therefore personal data) does not properly protect data subjects in all situations because it excludes situations where people can be individualized, tracked and profiled in an online environment. This loophole must be closed.
(2) **Ensure meaningful consent**. In order to ensure meaningful consent online, both the recitals as well as the definition of consent must be strengthened. Consent cannot be considered valid when data subjects have no real alternatives in the market, or in cases where consent is being used to legitimize excessive data processing. It is important to emphasize that consent can only be obtained for data processing that meets the requirement of proportionality; consent should never be used to legitimize excessive processing of personal data.
(3) **Limit use of legitimate interest ground**. The legitimate interest ground as proposed provides an unacceptable loophole for abusive or excessive processing. We propose to limit the use of this ground by introducing clear examples of what constitutes a legitimate interest. At the same time, data subjects need a stronger right to opt-out from processing based on this legal ground.
(4) **Prevent incompatible use of personal data**. Personal data collected for a specific purpose may only be used for other purposes that are compatible with the original purpose. This principle of purpose limitation is one of the fundamental pillars of data protection law and remains extremely important, especially in the online environment where data can be collected and re-combined rapidly and cheaply. We therefore propose to delete the proposed article which allows use of personal data for incompatible purposes.
(5) **Guarantee transparency and control.** Processing of personal data should always be transparent and understandable for data subjects. Data subjects deserve both accurate information about how their data is going to be processed as well as control over their personal information. Bits of Freedom proposes strengthening the rights to information, access and data portability as well as the obligation on the controller to provide privacy by default.
(6) **Prohibit furtive profiling**. Bits of Freedom is deeply concerned about the risks associated with profiling, especially online. We propose stronger limitations to the creation of profiles as well as limitations to the use of profiles for measures that affect data subjects. Finally, the right to information and access must be strengthened with respect to profiling.
(7) **Limit public interest exemptions**. The regulation contains too many exemptions for reasons of 'public interest'. These broad and vague grounds restrict the rights of the data subject (including erasure, to object and profiling), and the obligations of the controller regarding all the fundamental principles as well as regarding obligations on data breaches. We propose clarifying and limiting these grounds.

(8) **Improve data breach notification rules**. A data breach notification requirement should ultimately protect citizens by informing them when their data are accessed by unauthorized third parties. We propose to strengthen the definition and the notification regime itself in order to provide better protection to data subjects.

(9) **Strengthen privacy by design and default.** The concept of privacy by design and default must be strengthened and specified in order to provide meaningful protection to data subjects.

(10) **Properly define limitations to data protection rules.** Data protection rules should not prevail over other freedoms such as the right to freedom of expression or hinder the right to conduct scientific research. The boundaries of the Regulation must therefore be clear and understandable.

II Amendments to recitals				
Amendment	**Recital no.**	**Original version**	**Amendment**	**Explanation**
1. Territorial scope (article 3)	Recital 20	In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects, or to the monitoring of the behaviour of such data subjects.	In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services, **i<u>ncluding services offered free of charge</u>**, to such data subjects, or to the monitoring of the behaviour of such data subjects.	The Regulation must apply to all processing activities related to services, regardless of the fact whether or not these services are free of charge. This addition to Recital 20 ensures the applicability of the Regulation to so-called 'free services'.
2. Profiling (article 20)	Recital 21	In order to determine whether a processing activity can be considered to 'monitor the behaviour' of data subjects, it should be ascertained whether individuals are tracked **on the internet with data processing techniques which consist of applying a 'profile' to an individual**, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.	In order to determine whether a processing activity can be considered to 'monitor the behaviour' of data subjects, it should be ascertained whether individuals are tracked with **<u>the intention to use, or potential of subsequent use of</u>** data processing techniques which consist of applying a profile, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.	Consideration 21 unnecessarily narrows applicable law by defining monitoring behaviour as 'data processing techniques which consist of applying a 'profile' to an individual'. This would lead to non-applicability of the law in those cases where a controller is taking instant decisions on general categories, without 'knowing' the individuals affected. By deleting a part of this Recital, all tracking behaviour can be considered monitoring. By deleting the phrase 'on the internet' the recital becomes more technology neutral which may be relevant for profiling techniques that do not use the internet, such as camera surveillance or RFID tags in equipment used by data subjects. Finally, data collection and their use for profiling are not necessarily simultaneous. Data may be collected for one purpose in the first place, and could then afterwards be used for profiling.
3. Definition of data subject (article 4(1))	Recital 23	The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the	The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the	We have removed the word 'reasonably' in order not to narrow the scope of this recital unnecessarily. The addition

		means likely **reasonably** to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.	means likely to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable, **taking full account of the technological "state of the art" and technological trends**.	emphasizes the significant risk for the protection of personal data if developments in de-anonymisation are not fully taken into account.
4. Definition of data subject (article 4(1))	Recital 24	When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. **This may leave traces which, combined with unique identifiers and other information received by the servers**, **may be used to create profiles of the individuals and identify them. It follows that identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances.**	When using online services, individuals may be associated with **one or more** online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses, cookie identifiers **and other unique identifiers**. **Since these identifiers leave traces and can be used to single out natural persons, this Regulation should be applicable to processing involving such data, unless these identifiers demonstrably do no relate to natural persons, such as for example the IP addresses used by companies, which cannot be considered as 'personal data' as defined in article 4(2).**	The interservice version of this recital attempted to introduce a much broader definition of personal data, including unique identifiers and location data. Bits of Freedom proposes a stronger recital that leaves no doubt regarding the position of unique identifiers and their ability to link such information gathered via these identifiers to data subjects. Identifiers that have a close relation to a natural person must be regarded as personal data.
5. Definition of consent (article 4(8))	Recital 25	Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.	Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. **Informed consent should be facilitated insofar as possible by user-friendly information about the types of processing to be carried out.** Silence**, mere use of a service, or** inactivity **such as not un-ticking pre-ticked boxes,** should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.	Informed consent depends on information being freely available to the data subject in a user-friendly format. We also propose to include a reference to 'pre-ticked boxes' as these are frequently used online to obtain consent while not fulfilling the necessary consent conditions. It is a passive method of collecting consent which qualifies as 'opt-out' and which is often neither free nor informed.

6. Consent (article 7)	Recital 32	Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given.	Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given. **To comply with the principle of data minimisation, this burden of proof should not be understood as requiring positive identification of data subjects, unless necessary.**	It is important that obligations such as bearing the proof of consent, does not have the perverse effect of causing more data to be processed than otherwise have been the case.
7. Consent (article 7)	Recital 33	In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment.	In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment. **Consent can only be obtained for processing that is lawful and thus not excessive in relation to the purpose. Such disproportional data processing cannot be legitimized though obtaining consent.**	We have extended recital 33 in order to prevent the situation where a data controller complies with all the data processing 'formalities', but obtains consent for processing that is clearly disproportional. This should give regulators and judges an entry to evaluate substantive in addition to procedural fairness. Such a look beyond the procedural rules can also be found in general contract law, where principles like 'good faith' and reasonableness and fairness ultimately govern relations between parties in cases where specific terms of contract are found to breach these principles.
8. Consent (article 7)	Recital 34	Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.	Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context **or where a controller has substantial market power with respect to certain products or services and where these products or services are offered on condition of consent to the processing of personal data, or where a unilateral and non-essential change in terms of service gives a data subject no realistic option other than to accept the change or**	Many social media sites lead users to invest significant time and energy in developing online profiles. There would be a clear imbalance, in the sense of the Commission's proposal, in any situation where the user was given the choice between accepting new and unnecessary data processing and abandoning the work they have already put into their profile. Another case of clear imbalance would be if the market for the service in question is monopolistic/oligopolistic, so that the data subject does not in fact have a real possibility to choose an

			abandon an online resource in which they have invested significant time. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.	alternative service provider. Data portability would not fully address this issue, as it does not resolve the loss of the network effects in larger social networks.
9. Legitimate interest (article 6(1)(f))	Recital 38	The legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not **overriding**. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection. The data subject should have the right to object the processing**, on grounds relating to their particular situation and** free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.	**Under circumstances**, the legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not **overridden**. **Notably, direct marketing should not be seen as a legitimate interest**. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection. The data subject should have the right to object the processing free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.	This exception, as proposed by the European Commission, grants a very wide exception to data controllers to process data if *they* feel justified in undertaking such processing. This risks creating legal uncertainty and barriers to the single market. The European Data Protection Board should establish guidelines for acceptable “legitimate interests” in this context.
10. Purpose limitation (article 6(4))	Recital 40	The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for historical, statistical or scientific research purposes. **Where the other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject.** In any case, the application of the principles set out by this	The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for historical, statistical or scientific research purposes. In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes should be ensured.	This amendment reflects the amendment proposed to Article 6(4).

		Regulation and in particular the information of the data subject on those other purposes should be ensured.		
11. Data subjects rights (article 12)	Recital 47	Modalities should be provided for facilitating the data subject's exercise of their rights provided by this Regulation, including mechanisms to **request**, free of charge, in particular access to data, rectification, erasure and to exercise the right to object. The controller should be obliged to respond to requests of the data subject within a fixed deadline and give reasons, in case he **does** not comply with the data subject's request.	Modalities should be provided for facilitating the data subject's exercise of their rights provided by this Regulation, including mechanisms to **obtain**, free of charge, in particular access to data, rectification, erasure and to exercise the right to object. The controller should be obliged to respond to requests of the data subject within a fixed deadline and give reasons, in case he **can**not comply with the data subject's request.	This change stresses the rights of the data subjects, focusing on the outcome of them invoking their rights.
12. Right of information (article 14)	Recital 50	However, it is not necessary to impose this obligation where the data subject already disposes of this information, or where the recording or disclosure of the data is expressly laid down by law, or where the provision of information to the data subject proves impossible or would involve disproportionate efforts. **The latter could be particularly the case where processing is for historical, statistical or scientific research purposes; in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.**	However, it is not necessary to impose this obligation where the data subject already disposes of this information, or where the recording or disclosure of the data is expressly laid down by law, or where the provision of information to the data subject proves impossible or would involve disproportionate efforts.	The deleted text may be misunderstood as promoting a lower level of protection for certain kinds of data processing.
13. Right of access (article 15)	Recital 51	Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property **and in particular** the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.	Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property **such as** the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.	The proposed amendment clarifies what we believe to be the intention behind the Commission's proposal.
14. Transparent information	Recital 52	The controller should use all reasonable measures to verify the **identity of a data subject that requests** access, in particular in the context of	The controller should use all reasonable measures to verify the **authenticity of a subjects** access **request**, in particular in the context of	It is entirely possible that in some circumstances positive identification of the data subject would not be

(article 11) Right of access (article 15)		online services and online identifiers. A controller should not retain personal data for the unique purpose of being able to react to potential requests.	online services and online identifiers. A controller should not retain personal data for the unique purpose of being able to react to potential requests.	strictly necessary to provide access.
15. Right to be forgotten (article 17)	Recital 53	Any person should have the right to have personal data concerning them rectified and **a 'right to be forgotten' where the retention of such data is not in compliance with this Regulation**. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. **This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet.** However, the further retention of the data **should** be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.	Any person should have the right to have personal data concerning them rectified and **erased**. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. However, the further retention of the data **may** be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them, **provided the data are subject to adequate safeguards**.	The text proposed by the Commission is far too broad to be implemented "as is" without significant dangers for freedom of communication. The change in the first sentence relates to the proposed changes to article 17(2). Furthermore, as the rights being accorded to all citizens in this recital are comprehensive, there appears to be little specific value to demand "particular" attention for children. The text proposed by the Commission could have the perverse effect of implying a less than comprehensive protection for adults. Finally, further retention and processing of personal data should not be automatically permitted simply on the basis that they are being processed ostensibly for historical, statistical or scientific research processes. Such uses must be subject to adequate safeguards.
16. Right to be forgotten	Recital 54	**To strengthen the right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the**	*Deleted*	The text proposed by the Commission is far too broad to be implemented "as is" without significant dangers for freedom of communication. This deletion relates directly to the proposed changes to article 17(2).

		publication, where the controller has authorised the publication by the third party.		
17. Data portability (article 18)	Recital 55	To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. **This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract.**	To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used**, interoperable, and where possible open source** electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. **Providers of information society services should not make the transfer of those data mandatory for the provision of their services. Social networks should be encouraged as much as possible to store data in a way which permits efficient data portability for data subjects.**	The easier that it is to change providers, the less citizens will feel tied to a particular service, particularly if they are unhappy with the way their data is being used. As far as possible, the electronic formats used should interoperable and open source, in order to limit the use of proprietary formats which might be less useful for data subjects. However, providers should not make use of their services conditional on transferring data from previous service providers.
18. Profiling (article 20)	Recital 58	Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.	Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child. **Specifically, such processing should never, whether intentionally or not, lead to the discrimination of data subjects on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, or sexual orientation. Given the risk of discrimination, such processing should not be used in order to predict very rare characteristics.**	Adapted to reflect proposed amendments to Article 20.
19. Restrictions on principles and rights provided in the Regulation	Recital 59	Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of	Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related	It takes too long for egregious breaches of fundamental rights to be processed by the courts. An immediate review of the case by the Data Protection Board should help to eliminate abuses of this exception at

		the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union, and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.	obligations of the controllers may be imposed by Union or Member State law, as far as **strictly** necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union, and by the European Convention for the Protection of Human Rights and Fundamental Freedoms. **Any such measure should be notified to the Data Protection Board for an opinion which, if negative, should result in a referral to the Commission with view to starting an infringement procedure before the European Court of Justice.**	an early stage. If the Board comes to the conclusion that the measure is not compatible with the Regulation, it should inform the Commission, so that it can start proceedings against the Member State in question.
20. Privacy by design (article 23)	Recital 61	The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organizational measures are taken, both at the time of the design of the processing **and** at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default.	The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organizational measures are taken, both at the time of the design of the processing **and its underlying technologies as well as** at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default. **Data protection by design is the process by which data protection and privacy are integrated in the development of products and services through both technical and organisational measures. Data protection by default means that products and services are by default configured in a way that limits the processing and especially the disclosure of personal data. In particular, personal data should not be disclosed to an unlimited number of persons by default.**	“Privacy by design” can only be effective if it is correctly implemented at all stages in the design process. In order to achieve such implementation, the whole concept should be defined more clearly. This amendment proposes a more substantive definition of both “data protection by design” and “data protection by default”.

21. Representative in the EU (article 25)	Recital 63	Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring their behaviour, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of protection, or the controller is a **small or medium sized** enterprise or a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and may be addressed by any supervisory authority.	Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring their behaviour, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of protection, or the controller is a**n** enterprise or a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and may be addressed by any supervisory authority.	In the digital environment, it is no longer appropriate to use employee numbers as a measure of the size of a company. Instagram, a photo-manipulation company was recently purchased by Facebook for one billion dollars and had 13 employees at the time. What matters is the number of data subjects.
22. Research purposes (article 83)	Recital 126	Scientific research for the purposes of this Regulation should include fundamental research, applied research, and privately funded research and in addition should take into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area.	Scientific research for the purposes of this Regulation should include fundamental research, applied research, and privately funded research **in the meaning of Article 13 of the Charter of Fundamental Rights of the European Union** and in addition should take into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area. **It should not include market research.**	It should be clarified that the research exemption is meant for research in a strict sense, and not for market research.
III Amendments to articles				
23. Clarify applicability via territorial scope	Article 3	**Territorial scope** 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union. 2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour. 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.	**Territorial scope** 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union. 2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union**, irrespective of whether payment for these goods or services is required**; or (b) the monitoring of their behaviour. 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.	The notion of "processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union" could be clarified. This question has already been raised under the current framework (see e.g. Opinion of the Working Party 29 on applicable law). While under a Regulation, questions of applicable law become less complicated, there should still be explicit rules on the applicability of national law building on the Regulation, e.g. specific rules in the employment context (see Article 82). It should be clarified that controllers established outside the Union are

				also subject to the Regulation when offering goods or services without a payment (e.g. because the service is paid for by advertising) to data subjects in the Union.
24. Properly define the term 'data subject' to close loophole in protection	Art. 4(1)	**1. Definitions: data subject** 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;	**1. Definitions: data subject** 'data subject' means an identified natural person or a natural person who can be identified **or singled out**, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number **or a unique identifier**, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;'	The definition of personal data is currently too narrow as it excludes data which would not identify but would single out an individual data subject. Singling out means a data subject can be individualized or distinguished from other individuals, for example online, but not identified. Singling out of internet users through online identifiers is an important and very common activity which affects their privacy. Singling out or individualizing should therefore be subject to the provisions laid down in the Data Protection Regulation.
25. Define profiling	New article 4(3a)	*New article, to be inserted under Definitions.*	**Definitions: profiling** **'profiling' means any form of automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.**	We propose to define profiling in the definitions and not in article 20 of the Regulation. This definition separates the act of *profiling,* automated processing intended to evaluate a person, from the *measures* that are taken based on the results of this automated processing.
26. Strengthen consent for data processing	Article 4(8)	**Definitions: consent** 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes **by** which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;	**Definitions: consent** 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes which **proves that** the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;	By adding the requirement that consent must be provable by data controllers, the definition is better linked to section 7(1), which states that controllers bear the burden of proof for consent. It is vital to keep this definition and to strengthen it in this way, as it has to reflect the evolution in technologies that have become so sophisticated that people don't know or are not aware that their data is being collected and/or collated, and to what degree. There is ample evidence that current online

				consent-collecting methods, such as pre-ticked or opt-out boxes are neither free nor informed. Informed consent implies that data subject receive the information listed in Article 14 prior to the request for consent.
27. Improve definition of 'personal data breach'	Article 4(9)	**Definitions: personal data breach** 'personal data breach' means **a breach of security leading to** the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;	**Definitions: personal data breach** 'personal data breach' means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;	Personal data breaches can occur with or without a breach of security. Data breaches can for instance occur in cases where no security measures have been taken. Also, data breaches can occur without a breach of security: employees can for instance share data with unauthorized third parties. We therefore propose to define personal data breach as any accidental or unlawful destruction, loss or other 'hazards' occurring to the personal data.
28. Limit the use of the legitimate interest ground	Article 6(1)(f)	**Lawfulness of processing – legitimate interest** Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.	**Lawfulness of processing – legitimate interest** Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This **legal ground** shall not apply to processing carried out by public authorities in the performance of their tasks. **It shall also not apply to data processing that can also be based on one or several of the other grounds in this paragraph**.	Article 6(1)(f), as drafted by the Commission, can in practice offer controllers a way to avoid many processing restrictions altogether, since current experience suggests that few data subjects will be able or willing to test reliance on this criterion in court. Moreover, the broadness of the term “legitimate interest” creates legal uncertainty, both for data subjects and business. Furthermore this uncertainty will most probably lead to divergences in practice between different Member States and therefore a failure to achieve the goal of harmonisation. In the interest of legal certainty, it should at least be specified that direct marketing is not a legitimate interest in the scope of this Article, as the proposed amendment to recital 38 states, which would also remove inconsistencies with the revised ePrivacy Directive.

				If a data controller wishes to use "legitimate interest" as a basis for processing, this must be separately and explicitly flagged to the data subject and the data processor should publish its grounds for believing that its interests override those of the data subject. The amendment introduces obligations on controllers to this effect. As mentioned in recital 38, paragraph 1, point (f) should not apply to the processing carried out by public authorities. In the Commission proposal, it was unclear whether the last sentence of paragraph 1, point (f) referred only to the sentence before (i.e. the balancing test), or to the whole point. The proposed amendment clarifies this. For other controllers, this ground for lawfulness should only be used as a "last resort", with it being preferable to have processing based on one or several of the other grounds.
29. Controllers should document and inform about its legitimate interests	Article 6(3a)	*New article to be inserted after article 6(3)*	**In case of processing based on the legitimate interest ground referred to in point (f) of paragraph 1, the controller shall inform the data subject about this explicitly and separately. The controller shall also document the reasons for believing that its interests override the interests or fundamental rights and freedoms of the data subject.**	
30. Limit further processing to compatible purposes and prevent incompatible use	Article 6(4)	**Lawfulness of processing – further processing** **Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.**	*Deleted*	We propose deleting this section in order not to weaken the purpose limitation principle laid down in section 5(b) of the Regulation. This has also been suggested by the EDPS and the Article 29 Working Party. Further use of personal data must only be allowed for compatible purposes, and further guidance on what constitutes 'compatible' must

				be developed.
31. Strengthen consent by clarifiying that processing must always be proportionate		**Consent** 1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes. 2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter. . 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. 4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.	**Consent** 1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes. 2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. 4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller, **or where the obtained consent is not proportionate in relation to the purpose or purposes of the processing.**	Consent is too often perceived as a 'carte blanche'; because data controllers can obtain consent for processing that is not necessary for the performance of a contract or to serve a legitimate interest. Even though necessity is not a prerequisite, consent must always observe the principles related to data processing laid down in article 5 of the Regulation and must as a result always be necessary in relation to the purpose of collection. This amendment emphasizes that relation and provides extra protection for data subjects when they give their consent.
32. Improve information to data subjects; add information about profiling and data security	Article 14(1)	**Information to the data subject** Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information: (a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer; (b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); (c) the period for which the personal data will be stored; (d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;	**Information to the data subject** Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information: (a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer; (b) the **specific** purposes of the processing for which the personal data are intended **as well as information regarding the actual processing of personal data**, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller **as well as the reasons why the controller has concluded that this interest overrides the interests or fundamental rights and freedoms of the data subject** where the processing is based on point (f) of Article 6(1); (c) the period for which the personal data will be stored;	We propose a number of additions to the information that must be provided to data subjects when processing their personal data. All information requirements laid down in this article could be part of an online privacy policy that covers all aspects of the data processing undertaken by the data controller (not just the processing of personal data via the website and the use of cookies). Information must be written in clear and plain language and be easily accessible, in conformity with Article 11. In the first place, we consider it important that this information provides information about the actual processing of personal data that takes place. Secondly, we have included two extra categories of information, on profiling and on security measures.

		(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority; (f) the recipients **or categories of recipients** of the personal data; (g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission; **(h)** any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.	(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data; (e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority; (f) the recipients of the personal data; (g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission; **(h) where the controller processes personal data by automated means, as described in Article 20(1), information about the existence of processing for a measure of the kind referred to in Article 20(1) and the intended effects of such processing on the data subject.** **(i) information regarding specific security measures taken to protect personal data.** (**j**) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.	People must be informed when they are profiled, not just on request but by default. This will increase transparency and accountability of data controllers. Finally, we know from experience with the existing Directive that the "categories of recipients" wording leads to obtuse wording being used (such as "carefully selected third parties) which do nothing to increase transparency. We therefore proposed to learn from this experience and delete this wording.
33. Further improve information to data subjects	Article 14(8)	8. The Commission **may** lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	8. The Commission **shall** lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary**, as well as the needs of the relevant stakeholders, including the possible use of layered notices**. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	In the interest of clarity and uniformity, the elaboration of standard format should be mandatory instead of optional. The development of these forms should be carried out with input from the relevant stakeholder, including designers and behavioural economists. Given that layered notices can be a way to provide appropriate information in a variety

				of formats, including on mobile devices (where long statements are harder to read), they should be specifically mentioned.
34. Improve right of access for data subjects; include access to use of data statistic use, logic behind profiling as well as to information about disclosures to public authorities	Article 15	**Right of access for the data subject** 1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients **or categories of recipients** to whom the personal data are to be or have been disclosed, in particular to recipients in third countries; (d) the period for which the personal data will be stored; (e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data; (f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority; (g) communication of the personal data undergoing processing and of any available information as to their source; (h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20. 2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic	**Right of access for the data subject** 1. The data subject shall have the right to obtain from the controller at any time, on request, **in clear and plain language**, confirmation as to whether or not personal data relating to the data subject are being processed, **and as to whether the controller takes measures in respect of the data subject that are based on profiles as referred to in Article 20(1). This shall also apply to data which only permit singling out, where the data subject can verifiably authenticate him/herself.** This should also apply for non-personally identified data, where the data subject can verifiably identify him/herself. Where such personal data are being processed **or such measures are taken**, the controller shall provide the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients to whom the personal data are to be or have been disclosed to**, including all** recipients in third countries; (d) the period for which the personal data will be stored; (e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data; (f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority; (g) communication of the personal data undergoing processing and of any available information as to their source;	We have strengthened the Article about access rights by adding a number of requirements that will give data subject more control over their personal data. Firstly, the requirement in paragraph (1) to provide information in clear and plain language, introduced in Article 11(2), also applies to the information provided following an access request. The second amendment in that paragraph allows an individual data subject to personally authentify him/herself in order to gain full rights to the data collected on him/herself. Secondly, under subparagraph (c) we propose to allow access to the real recipients of personal data instead of the categories of recipients, in order to allow data subjects to effectively address third party recipients where necessary. Subparagraph (i) proposes access to information about data processing for historical, statistical and scientific purposes, while subparagraph (j) provides information about the logic behind automated processing of personal data, including access to the logic underpinning such automated processing. This will allow data subjects to effectively challenge measures taken as a result of automated processing. Finally, subparagraph (k) informs data subjects about the request for their personal data as well as the possible disclosure of such data to

		form, unless otherwise requested by the data subject. 3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1. 4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20. **(i) where applicable, in what manner and for what specific purposes the data will be processed for statistical purposes and how will be ensured that data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information;** **(j) the logic underpinning the data undergoing processing in case of processing referred to in Article 20.** **(k) in case of disclosure of personal data to a public authority as a result of a public authority request for personal data, a confirmation of the fact that such a request has been made, information about whether or not the request has been fully or partly complied with and an overview of the data that were requested or disclosed.** 2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject. 3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1. 4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various	governmental organizations as a result of a governmental request. As people's lives shift increasingly to the internet, governments increasingly turn to requesting user data from internet services. In order to protect the privacy of data subjects we propose to extend the right of access to information on whether such a request has been made and by which governmental organization, if it was complied with in whole or in part and which data were disclosed following the request.

			sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	
35. Improve the right to data portability	Article 18	**Right to data portability** 1. The data subject shall have the right, where personal data are processed by electronic means **and in a structured and commonly used format**, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject. 2. Where the data subject has provided the personal data **and the processing is based on consent or on a contract**, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn. 3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	**Right to data portability** 1. The data subject shall have the right, where personal data are processed by electronic means, to obtain from the controller a copy of data undergoing processing in an electronic, **interoperable** and structured format which is commonly used and allows for further use by the data subject. 2. Where the data subject has provided the personal data, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn. **2a. This right is without prejudice to the obligation to delete data when they are no longer necessary under Article 5(e).** 3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	The applicability of the right to data portability should be extended to cases beyond processing based on contract or consent. Similarly, controllers should not have the possibility to deny making the data available by claiming that the format used is not “commonly used”. It should be clarified that this right is without prejudice to the obligation to delete data when they are no longer needed.
36. Strengthen the right to object to data processing when based on legitimate interest	Article 19 (1) and (2)	**Right to object** 1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) **and (f)** of article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which	**Right to object** 1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d) **and** (e) of article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which	We propose to extend the right to object free of charge and without demonstrating a 'particular situation' for all forms of data processing based on article 6(f). This is necessary to restore the balance between the interests of the data

		override the interests or fundamental rights and freedoms of the data subject. 2. Where personal data **are processed for** direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.	override the interests or fundamental rights and freedoms of the data subject. 2. Where personal data **processing is based on article 6(1)(f)**, the data subject shall have the right to object free of charge **at any time including at the time of the collection of their data**, to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject **at least via the same channel that is used to collect the data,** in an intelligible manner **using clear and plain language, adapted to the data subject,** and shall be clearly distinguishable from other information.	controller and data subject.
37. Stricter rules for profiling and more protection for data subjects where profiling takes place	Article 20	**Measures based on profiling** 1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour. 2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if **the processing**: (a) **is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where** suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or (b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to	**Profiling and measures based on profiling** 1. Every natural person shall have the right**, both off- and online,** not to be subject to **profiling or** a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely **or predominantly** on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour. 2. Subject to the other provisions of this Regulation, **including paragraph 3 and 4,** a person may be subjected to **profiling or** a measure of the kind referred to in paragraph 1 only if **such**: (a) **is necessary for the performance of a contract to which the data subject is a party or for the implementation of pre-contractual measures taken at the request data subject, provided that** suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention **including the right to an explanation of the decision reached after such an intervention;** or (b) is expressly authorized by a Union or Member State law which also lays down suitable measures	Profiling of data subjects is a form of automated processing that has become increasingly more popular over the last years. The decreasing cost of data storage and the fact that automated processing of personal data has become much easier, has lead to the use profiling software by both private parties and government institutions. Profiling is often furtive; it takes place without data subjects being aware of it. Especially the online environment allows for the creation of profiles of data subjects based on their behavior, through cookies, device fingerprinting or other means of gathering of user data. In order to mitigate the negative effects of profiling on the privacy of data subject we propose to strengthen article 20. We have strengthened paragraph 2(a) by bringing it in line with the Council of Europe's recommendation on this subject. Furthermore we have increased legal safeguards against discriminatory practices in paragraphs 2(b) and 2(c). While profiling is in some circles seen as a panacea for many problems, it

		suitable safeguards. 3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not **be based solely on** the special categories of personal data referred to in Article 9. **4.** In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject. **5**. The Commission shall **be empowered to** adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.	to safeguard the data subject's legitimate interests **and which protects data subjects against possible discrimination resulting from the measures described in paragraph 1**; or (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards, **including effective protection against possible discrimination resulting from measures described in paragraph 1.** **3.** Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not **include or generate any data that fall under** the special categories of personal data referred to in Article 9**, except when falling under the exceptions listed in Article 9(2).** **4. Profiling that (whether intentionally or otherwise) has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, or sexual orientation, or that (whether intentionally or otherwise) result in measures which have such effect, shall be prohibited.** **5. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be used to identify or individualize children.** **6**. In the cases referred to in paragraph 2, the information to be provided by the controller under Articles 14 **and 15** shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject, **as well as the access to the logic underpinning the data undergoing processing.** **7**. **Within six months of the entry into force of this Regulation,** the Commission shall adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and	should be noted that there is a significant body of research addressing its limitations. Notably, profiling tends to be useless for very rare characteristics, due to the risk of false positives. Also, profiles can be hard or impossible to verify. Profiles are based on complex and dynamic algorithms that evolve constantly and that are hard to explain to data subjects. Often, these algorithms qualify as commercial secrets and will not be easily provided to data subjects. However, when natural persons are subject to profiling, they should be entitled to information about the logic used in the measure, as well as an explanation of the final decision if human intervention has been obtained. This helps to reduce intransparency, which could undermine trust in data processing and may lead to loss or trust in especially online services. There is also a serious risk of unreliable and (in effect) discriminatory profiles being widely used, in matters of real importance to individuals and groups, which is the motivation behind several suggested changes in this Article that aim to improve the protection of data subjects against discrimination. In relation to this, the use of sensitive data in generating profiles should also be restricted.

			conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2(b). **The Commission shall consult representatives of data subjects and the Data Protection Board on its proposals before issuing them.**	
38. Clarify and limit the public interest exemptions	Article 21(1)	**Restrictions** 1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11 to **20** and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard: (a) public security; (b) the prevention, investigation, detection and prosecution of criminal offences; (c) other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters **and the protection of market stability and integrity**; (d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; **(e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a), (b), (c) and (d);** (f) the protection of the data subject or the rights and freedoms of others. 2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least as to the objectives to be pursued by the processing **and** the determination of the controller**.**	**Restrictions** 1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11 to **19** and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard: (a) public security; (b) the prevention, investigation, detection and prosecution of criminal offences; (c) other **important** public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters; (d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; (**e**) the protection of the data subject or the rights and freedoms of others. 2. In particular, any legislative measure referred to in paragraph 1 **must comply with the standards of necessity and proportionality and** shall contain specific provisions at least as to**:** **(a)** the objectives to be pursued by the processing**;** **(b)** the determination of the controller**;** **(c) the specific purposes and means of processing;** **(d) the categories of persons authorised to process the data;** **(e) the procedure to be followed for the processing;** **(f) the safeguards against any arbitrary**	Point (e) of paragraph 1 is unduly wide; legitimate derogations are already covered by points (a) to (d). The other changes bring the possible restrictions more in line with the current restrictions permissible under Directive 95/46/EC. For the additional safeguards in paragraph 2 and the new paragraph 3 see also the EDPS opinion on the data protection reform package, points 159-165. Paragraph 4 gives effect to the new procedure proposed in recital 59.

			interferences by public authorities; **(g) the right of data subjects to be informed about the restriction** **3. Legislative measures referred to in paragraph 1 shall not impose obligations on private controllers to retain data additional to those strictly necessary for the original purpose.** **4. Legislative measures referred to in paragraph 1 shall be notified to the European Data Protection Board for opinion. If the European Data Protection Board considers that the notified measure does not comply with the requirements of paragraph 2, it shall inform the Commission. The Commission shall then consider launching the procedure established under Article 258 of the Treaty on the Functioning of the European Union.**	
39. Strengthen data protection by design and default	Article 23	**Data protection by design and by default** 1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate **technical and organisationa**l measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. 2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals. 3. The Commission shall be empowered to adopt	**Data protection by design and by default** 1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate-measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. **This shall include both:** **(a) technical measures relating to the technical design and architecture of the product or service; and** **(b) organisational measures which relate to the operational policies of the controller.** **Where a controller has carried out a data protection impact assessment pursuant to Article 33, the results of this shall be taken into account when developing the measures referred to in points (a) and (b) of this paragraph.** 2. The controller shall implement mechanisms for ensuring that, by default, only those personal data	The concept of “data protection by design” needs more specification. Given that in many services such as social networks, the default settings allow wide public sharing of information, the requirements in paragraph 2 should be strengthened.

		delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services. 4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. **This shall be ensured using technical and organisational measures, as appropriate.** In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals **and that data subjects can control the distribution of their personal data**. 3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services. 4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	
40. Delete the SMEs exemptions and replace by record-criterion	Article 25	**Representatives of controllers not established in the Union** 1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union. 2. This obligation shall not apply to: **(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or** (b) an enterprise **employing fewer than 250 persons** ; or (c) a public authority or body; or	**Representatives of controllers not established in the Union** 1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union. 2. This obligation shall not apply to: (**a**) an enterprise **holding less than 250 records containing personal data relating to individuals**; or (**b**) a public authority or body; or (**c**) a controller offering only occasionally goods or services to data subjects residing in the Union, **providing it holds less than 250 records**	The current wording of Article 25 states that businesses with less than 250 employees do not have to appoint a representative in the EU. This exception would make effective enforcement very difficult, if not impossible, causing a major loophole. Smaller companies can hold enormous numbers of records and should therefore appoint a representative in the EU in order to allow for effective enforcement of the Regulation. Without such a representative, a European DPA would have to go to a court in its own country to ask for confirmation

		(d) a controller offering only occasionally goods or services to data subjects residing in the Union. 3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside. 4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.	**relating to individuals residing in the Union.** 3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside. 4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.	of its jurisdiction if the data controller does not comply. This is extremely time consuming as well as ineffective, as nothing prevents a data controller from going to a court in its own place of residence asking for a contradictory ruling. We suggest to base the representation of the number of records held by a data controller. A record may relate to an employee, a customer, a prospect or a natural person in any other quality. The amount of personal data being processed should be the determining factor, not size of enterprise.
41. Aggregated publication of governmental requests for personal data	*Article 28a*	*New article, to be inserted after Article 28*	**Publication of public authority requests** **1. Each controller shall, at least annually, publish an aggregated overview of requests by a public authority for disclosure of personal data in the past reporting year. Such an overview shall include per country:** **(a) the total number of received requests;** **(b) the total number of data subjects affected by these requests; and** **(c) the number of requests that the data controller has fully or partly complied with.** **2. The controller shall publish the overview referred to in paragraph 1 in a transparent and easily accessible manner.**	Data requests by public authorities to private organisations are increasing, especially in the online environment. The potential for abuse of this power is enormous, and at the meantime there is a serious chilling effect created by uncertainty over the exercise of these powers. In order to protect the privacy of data subjects and increase transparency about such governmental requests, we propose a publication requirement for data controllers to inform data subjects about such requests. Next to this new article which allows for the provision of aggregated data, we propose to extend the right of access of data subjects (amendment no. 34) to receive information about requests made by governments regarding their personal data.
42. Make personal data breach notifications publicly accessible	*New article 31(5)*	*New article 31(5), to be inserted after 31(4)*	**6. The supervisory authority maintains public register of all notified data breaches which can be accessed free of charge.**	A public register of data breaches notified to data protection authorities allows data subjects, security experts, journalists and policy makers to examine personal data

				breaches over time. It will provide insights to the scope of personal data breaches in certain sectors and allow policy makers to base their policymaking on these facts and figures. The Commission shall lay down further rules to determine which information must be made accessible.
43. Improve notification of personal data breach to data subjects	Article 32	1. **When the** personal data breach **is likely to adversely affect the protection of the personal data or privacy of the data subject**, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay. 2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points **(b) and (c)** of Article 31(3). **3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.** **4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.** 5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1. 6. The Commission may lay down the format of the communication to the data subject referred to	1. **In case of a** personal data breach, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay. 2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points **(a) to (e)** of Article 31(3). **The communication to the data subject shall furthermore, taking into account the nature of the personal data breach, the consequences of the breach the number of data subjects invloved and the costs of such communications, contain all information necessary to guarantee provision of fair and accurate information.** **3**. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1. **4**. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 **and 2** and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	Bits of Freedom proposes an extension of the requirement to notify all personal data breaches to data subjects involved, regardless of whether the data breach 'adversely affects' the data subject. In the first place because it is hard to imagine how data subjects could be affected in a non-adverse way. Secondly, because data controllers cannot determine what the impact of a data breach is on a specific data subject. By notifying the breach fully and directly to data subjects instead of to the supervisory authority, affected data subjects can immediately take precautions where necessary. Furthermore, we propose to notify personal data breaches also in cases where information was renderend unintelligible, unless the data is encrypted, the encryption cannot be reversed without the encryption key, provided that the key was not affected by any breach.

		in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).		
44. Preserve the freedom of expression by creating a wider exemption	Article 80	**Processing of personal data and freedom of expression** 1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organisations in Chapter V, the independent supervisory authorities in Chapter VI and on co-operation and consistency in Chapter VII **for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression** in order to reconcile the right to the protection of personal data with the rules governing freedom of expression. 2. Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment law or amendment affecting them.	1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organisations in Chapter V, the independent supervisory authorities in Chapter VI and on co-operation and consistency in Chapter VII **whenever this is necessary** in order to reconcile the right to the protection of personal data with the rules governing freedom of expression. **1a. The European Data Protection Board shall issue guidance on when such exemptions or derogations may be necessary, after consultation with representatives of the press, authors and artists, data subjects and relevant civil society organisations.** 2. Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment law or amendment affecting them.	It is not always clear when an exercise of the freedom of expression qualifies as “journalistic” or “artistic”. Consider the example of publishing information about human rights violations by NGOs, which may have been obtained in breach of data protection rules.
45. Narrow down the justitications for processing for research purposes	Article 83	1. Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if: (a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject; (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner. 2. Bodies conducting historical, statistical or	1. Within the limits of this Regulation, personal data n**ot falling within the categories of data covered by Articles 8 and 9** may be processed for historical, statistical or scientific research purposes only if: (a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject; (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner.	The justifications for the processing of personal data for historical, statistical and scientific research purposes needs to be narrowed down and described into more detail in order to prevent the existence of a wide exemption for data processing for all different kinds of 'research purposes'. We propose to narrow down the legal ground on which such processing can take place, and advocate a more specific description of 'research purposes' in recital 126, allowing

		scientific research may publish or otherwise publicly disclose personal data only if: (a) the data subject has given consent, subject to the conditions laid down in Article 7; (b) the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests; or (c) the data subject has made the data public. 3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the processing of personal data for the purposes referred to in paragraph 1 and 2 as well as any necessary limitations on the rights of information to and access by the data subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances.	**2. Subject only to the exception in paragraph (3), data falling within the categories of data covered by Articles 8 and 9 of the Regulation may be processed for historical, statistical or scientific research only with the consent of the data subjects, given in accordance with Article 4(8).** **3. Member States may by law provide for exceptions to the requirement of consent for research, stipulated in paragraph (2), with regard to research that serves exceptionally high public interests, if that research cannot possible be carried out otherwise. The data in question shall be anonymised or pseudonymised to the highest possible standards, and all possible measures shall be taken to prevent re-identification of the data subjects. Such processing shall be subject to prior authorisation of the relevant national supervisory authority or authorities, in accordance with Article 34(1) of this Regulation, and to the Consistency Mechanism provided for in Chapter VII, Section 2, of this Regulation.** 4. Bodies conducting historical, statistical or scientific research may publish or otherwise publicly disclose personal data only **with the consent of the data subjects, given in accordance with Article 4(8).** 3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the processing of personal data for the purposes referred to in paragraph 1 and 2 as well as any necessary limitations on the rights of information to and access by the data subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances.	