European Parliament

Data protection rules applicable to the European Parliament and to MEPs

Current regime and recent developments

SUMMARY

Data protection is a fundamental right enshrined in both primary and secondary EU law. More specifically, the main reference for data protection in Europe is the 2016 General Data Protection Regulation (GDPR), which is fully applicable since 25 May 2018. Moreover, specific data protection rules (currently Regulation 45/2001) apply to the EU institutions. The latter are under review, to adapt their principles and provisions to the GDPR. The processing of data relating to parliamentary activities is therefore covered by these specific rules, as is personal data relating to, or processed by, Members of the European Parliament (MEPs).

This Briefing provides an overview of the main provisions applicable to parliamentary activities and in particular to MEPs, taking account of the fact that the process of reforming the current rules has not been formally concluded (even if a political agreement has been reached between the co-legislators). An update of this Briefing will be published in due course.

Introduction

The rights to private life and to data protection are enshrined in Articles 7 and 8 of the Charter of Fundamental Rights (CFR), binding as EU primary law since the Lisbon Treaty. Data protection is also enshrined in Article 16 of the Treaty on the Functioning of the EU (TFEU), which constitutes a specific legal basis for adopting legislative acts on data protection.[1] Article 52(3) CFR, states that the meaning of the rights guaranteed in the Charter is the same as in the European Convention on Human Rights (ECHR): Article 8 of the latter protects the right to a private life (interpreted in jurisprudence as including the right to data protection), which can be subject to certain restrictions only if 'in accordance with law' and 'necessary in a democratic society'.

The advance of digital technologies and the emergence of 'big data' and of a data-driven society – where almost every daily activity involves the flow and combination of data – require clear and up-to-date rules, suited to the digital era. The collection and processing of data for many different purposes – often automatically – offer undeniable benefits for individuals and society, but also raise concerns for individual rights and freedom, including privacy, non-discrimination and freedom of information. The EU has a long tradition of data protection rules: at the level of secondary law, it adopted its general rules in the 1990s. Their update is also necessary due to technological advances.

EU institutions and bodies are not exempt from data protection rules and principles, but are subject to specific rules. In fact, in contrast to what happens at national level, ad hoc rules on data processing within the EU institutions have existed since Regulation No 45/2001, which is now under review, as discussed below. Data processing relating to the activities of the European Parliament is thus subject to these rules.

Authors: Shara Monteleone and Silvia Kotanidis
Members' Research Service

PE 623.540 – June 2018

The purpose of this Briefing is to provide an overview of the data protection framework applicable to the European Parliament and its individual Members (MEPs). It takes into account recent developments in the European data protection legal framework – namely, the General Data Protection Regulation (GDPR) and the specific regime applicable to EU institutions and bodies. After a brief discussion of the current law, this Briefing analyses how its revision applies to the parliamentary sphere, both at the level of the European Parliament and of its individual Members and parliamentary groups. It also considers open issues that need to be addressed.

General Data Protection Regulation (GDPR)

Aimed at strengthening citizens' rights uniformly, while reducing burdens for companies and public organisations, the GDPR entered into force in 2016. It repeals Directive 95/46/EC, and since 25 May 2018 it has been **fully applicable** to individuals, as well as to private or public organisations processing personal data. It is, therefore, the main reference for data protection in Europe. The GDPR contains general principles and rules (e.g. conditions for lawful data processing, obligations and rights deriving from data processing and safeguards) and calls for Regulation 45/2001 to be adapted to its stronger rules.[2] For this reason, a new regulation repealing the 2001 rules has been proposed (hereinafter '*new* Regulation 45/2001').[3]

GDPR: an overview

Defined as an evolution, rather than a revolution, the GDPR (Rapporteur: Jan Albrecht, Greens/EFA, Germany) builds on its 1995 predecessor, Directive 95/46/EC and on the case law of the Court of Justice (CJEU), which has on several occasions underlined the importance of a high level of data protection for a democratic society. It was adopted as part of a wide-ranging reform package, which also includes a directive on data processing for law enforcement purposes. As a regulation, it is directly applicable in the Member States, although they have some discretion.

As for its material and territorial **scope**, the GDPR applies to the processing of personal data, including by automated means. It excludes: data processing carried out outside the scope of EU law (e.g. national security), or for purposes of crime prevention or investigation, or by an individual as part of a purely personal or household activity.

The GDPR applies to **data controllers** (i.e. natural or legal person, responsible for processing personal data and deciding on the purposes of the processing) operating in the EU, wherever they are based.

Data is considered personal when it can identify a person (including ID card number, IP address, phone location data). The rules do not apply to anonymous / anonymised data. Data processing is allowed if some conditions are satisfied, i.e. with the subject's informed and *unambiguous consent* or on other legal grounds (e.g. the performance of a contract; a legal obligation; or legitimate interests overriding the fundamental rights of the subject). Also, data must be collected for specified, explicit and legitimate purposes and not further processed in an incompatible way. The GDPR, save exceptions, prohibits the processing of special data (e.g. revealing ethnic origins, political or religious beliefs, or details on individual's health or sex life).

Besides strengthening individuals' existing **rights** (e.g. to have clearer information on data usage, as well as easier access to one's data), the GDPR introduces new rights, such as the transfer of personal data from one service provider to another (*data portability*); the right to have one's data deleted if there are no legitimate grounds for retaining them (the *right to be forgotten*); the right to *object to profiling* (as statistical deduction is often used to make predictions about people).

The GDPR has increased **accountability** but has also reduced the burden for data controllers. The latter have to inform individuals of the purposes and use of data and are responsible for demonstrating their compliance with the rules. They have to keep a record of their data-processing activities rather than notifying the national authority of the processing activity; they must take technical and organisational measures to make data secure, and inform both individuals and the competent authority, if data are *accidentally or unlawfully* destroyed or accessed by unauthorised persons (*breach notification*). Requirements, under *certain circumstances*, include: designation of a data protection officer, impact assessment, and data protection by design and by default (i.e. 'to embody' data protection rules within a product or service).

As for **sanctions**, fines of *up to* 4 % of a firm's *total worldwide annual turnover* may accompany or replace corrective measures (such as warnings or orders) adopted by national supervisory authorities (DPAs) in the case of some infringements. As for the remedies, data subjects can lodge a claim before empowered DPAs or national courts. At EU level, a new board for national supervisory authorities has been established (EDPB).

Data transfers to third countries may take place (as in the 1995 directive) only if the third country can ensure an adequate level of data protection. According to the CJEU, limitations to data protection rights are justified only if provided in law, if strictly necessary and proportionate.

The Commission published a communication on GDPR implementation and an online tool for businesses. The Article 29 Working Party (an independent European advisory body) also provided guidelines, including on consent, profiling and transparency.

Rules for EU institutions: Regulation 45/2001 and its reform

Main aspects of current Regulation 45/2001

At present, the rules on personal data processed by EU institutions are set out in Regulation No 45/2001 (at least until its revision is complete), which applies, with some specificities, the main principles of the 1995 General Data Protection Directive. Its objectives are to ensure individuals' rights and to allow the free flow of personal data between Member States and the institutions and among the institutions themselves, supported by an effective independent supervisory system. It lays down rules similar to those defined in the general directive, such as the requirements for lawful processing: necessity in relation to a legal basis, such as the performance of a task carried out in the public interest on the basis of the EU law or in the legitimate exercise of official authority vested in the institution, for compliance with legal obligations, for the performance of a contract, or the subject's consent. Data should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;[4] moreover, they should be kept for no longer than necessary for the same purposes, except for historical, statistic or scientific purposes, in which case longer periods are allowed providing data are anonymised or encrypted. A change in purpose is permitted if expressly set by internal rules of the institution or body.

Actors

The actors involved are: the **data subject**, i.e. the person whose data are collected, stored or otherwise processed (thus, any citizen whose data are processed by a EU institution as well as each of its staff *and each MEP)*; the **data controller**, which, under Regulation 45/2001, is the *EU institution or body*, the *directorate-general, the unit or any other entity (potentially including MEPs and political groups)* which, alone or jointly with others, determines *how* and for what *purposes* data are processed; the controller is also the entity that receives requests from data subjects to exercise their rights; the **data processor**, i.e. the natural or legal person or public body processing data on behalf of the controller; the **data protection officers** (DPOs), i.e. the officials responsible in *each* institution and body to ensure the internal application of the 2001 provisions and that data subjects' rights are not likely to be adversely affected by the processing operations; and the **European Data Protection Supervisor** (EDPS), the independent supervisory authority that ensures the application of the same rules across all the EU institutions and who liaises with the DPOs. The EDPS was established by Regulation 45/2001, which specifies the powers to be exerted and duties to be carried out in total independence. These include: *supervision and enforcement* powers, conducting prior checks and investigating complaints lodged by data subjects, conducting inquiries and monitoring the application of the rules by a EU institution or body – with the exception of the Court of Justice of the European Communities 'acting in its judicial capacity' (Article 46); *consultation* (advising data-subjects and the EU institutions); and *cooperation* (with data protection authorities).[5]

Obligations and rights

Data **controllers** have the obligation to **inform** the data subject;[6] to maintain accurate and updated data; to pay particular attention to **special** categories of **data**, i.e. 'sensitive' data (e.g. ethnic origin, political opinions, religious beliefs, trade union membership, health and sex life);[7] to **delete** or block data if no longer needed for the original purpose; to make data accessible to the data subject; to ensure the technical and organisational security of personal data; and to respond (within 15 working days) to data subjects' requests regarding the exercise of their **rights**, e.g. the right to access, rectification, blocking, erasure, and to object to processing of personal data.[8] The institutions or bodies, as data controllers, may **restrict** these rights when *necessary* for: crime prevention, investigation or prosecution; national security, public security or defence of a Member State; an important economic or financial interest.

Moreover, the regulation provides for the mandatory appointment of a **DPO** within *each* EU institution, to ensure that the rules are applied and to advise data controllers. A general **notification** procedure is required under the current 2001 rules, meaning that the data controller has to contact and inform the DPO prior to undertaking a processing operation: the DPO keeps a *register of data processing operation*s and can investigate matters related to the tasks. The DPO has to consult the EDPS (**prior checks)** when processing operations are likely to present risks to subjects' rights.

Moreover, the DPO's powers and duties are currently indicated in Annex of Regulation 45/2001 and in the 2005 European Parliament Bureau Decision implementing it. In particular, the DPO (who must be independent in performing his or her tasks) may make recommendations to the institution and to the controller concerned, may *investigate matters* and occurrences relating to his or her tasks; he or she shall have *access at all times* to the data being processed and to all offices and data processing installations; and every controller concerned shall assist him or her.[9]

As for the sanctions, any failure to comply with the obligations provided in Regulation 45/2001, whether intentionally or through negligence, may make an official or servant of the EU institutions liable to **disciplinary action** (according to the Staff Regulations of officials of the EU institutions).[10]

The boxes below provide examples of application of the current rules.

Parliamentary questions and personal data

Parliamentary questions may in certain circumstances pose problems for the protection of personal data. Such conflicts may arise, for instance, for the content of questions for oral answer (Rule 128 of the Rules of Procedure), questions for written answer (Rule 130 of the Rules of Procedure), minor interpellations for written answer (Rule 130a of the Rules of Procedure), and major interpellations for written answer with debate (130b of the Rules of Procedure) that may contain personal information. Also in such cases, the protection of personal data enshrined in Regulation 45/2001 remains of primary importance, notwithstanding the fact that Members, for instance under Rule 130, in submitting questions for written answer to the President of the European Council, the Council, the Commission or the Vice-President of the Commission/High Representative of the Union for Foreign Affairs and Security Policy, are legitimately expressing their political opinion and therefore enjoy freedom of speech in the exercise of their parliamentary mandate. These situations fall under Regulation 45/2001, which protects personal data. The practice established within the European Parliament entails that, where personal data risk being disseminated via parliamentary questions, without the consent of the data subject, the Parliament's administration ensures that unlawful processing is avoided by proposing the anonymisation of certain data, save where exceptions under Regulation 45/2001 apply. In the case of disagreement, the President of Parliament is competent to ultimately decide on the admissibility of the question.

The Member's declaration of financial interests

For reasons of transparency and to enhance integrity in the execution of the Member's mandate, Article 4 of the Code of Conduct for Members of the European Parliament, now Annex I of the Rules of Procedure, requires Members to submit a declaration of financial interests to the President of the EP. This declaration must contain specific financial information, such as income from the Member's occupation for three years prior to taking up office, including membership of company boards or any other remuneration for occasional outside activities exceeding €5 000 per year. MEPs must indicate if activities are remunerated and, if so, the income bracket to which the remunerations belong (e.g. €1 to €499; €500 to €1 000, etc.). An important aspect of the declaration of financial interests is the requirement that such information be published on the EP's website in an easy and accessible manner (Article 4(3) of the Code of Conduct). This publication of personal data is justified under the exception provided in Article 5(a) as it is necessary for the performance of Parliament's tasks in the public interest, on the basis of its Rules of Procedure.

Petitions and protection of personal data

The right to petition is a right guaranteed by Articles 24 and 227 of the TFEU and serves citizens' democratic participation. The Rules of Procedure of the European Parliament (Rules 215 to 217) provide that petitions become public documents once registered, with the possibility to withhold the name of the petitioner to protect his or her privacy. Case T-343/13 concerned an action for damages against the European Parliament on the grounds that information regarding the petitioner's health, his son's health and his professional life was unlawfully disseminated and not erased in due time, contrary to Regulation 45/2001. The General Court in its judgment decided in favour of the European Parliament, considering that the petitioner had given his free and informed consent to the processing of his personal data, including sensitive data (Articles 5 and 10 of Regulation 45/2001) since the information made available on Parliament's website ('online help') could enable a reasonably observant petitioner to assess the full extent of the implications of his/her action in submitting the petition. The consent was also specific and express as it was given through a specific form that the petitioner ticked in the affirmative. Therefore, the dissemination of personal data by the Parliament was not unlawful. As to the erasure of personal data from the web, the General Court considered that Parliament had no binding obligation to erase and the long time that elapsed before full erasure could be achieved was not a violation of Regulation 45/2001. This case, as the General Court observed, differed from the *Google* case (C-131/12) on the 'right to be forgotten', where the data subject did not consent to the initial publication of his data.

Donations

Other data protection rules of relevance to parliamentary activities can be found in Regulation 1141/2014 on the statute and funding of European political parties and foundations. Article 33 states that, in processing data pursuant to this regulation, the Parliament is considered a data controller and shall comply with Regulation 45/2001, while, for the same purposes, the European political parties shall, instead, comply with Directive 95/46/EC and with national provisions (now presumably with the GDPR). On the need to strike a balance between the right to data protection and the interests of transparency, Article 20 of Regulation 1141/2014 states that the names of donors and their donations not exceeding €1 500 per year should not be published.

Main changes in the regulation that will replace Regulation 45/2001

Together with other initiatives in the field of data protection, in January 2017 the Commission adopted a proposal for *a regulation on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, [offices and agencies] and on the free movement of such data, and repealing Regulation (EC) No 45/2001*.[11] The aim was to reform the existing 2001 rules to align them to the 2016 GDPR, that is to ensure that EU institutions and bodies processing personal data comply with a coherent and up-to-date framework ensuring free movement of data among services (or to recipients in the EU), while upholding individuals' rights in accordance with the GDPR as well as with the e-Privacy rules (also currently under review).

The new regulation that will replace Regulation 45/2001: legislative process

The proposal was published in January 2017. A compromise text (political agreement) between the co-legislators was reached in May 2018 on equivalent rules on data protection in the EU institutions.

Within the European Parliament, the proposal was assigned to the Civil Liberties Committee (LIBE). The Committee report (rapporteur: Cornelia Ernst, GUE/NGL, Germany), put forward several amendments, aimed at harmonising the data protection regime also for EU bodies carrying out activities in the field of *judicial cooperation in criminal matters* and *police cooperation*. Parliament's LIBE committee adopted its report and the mandate to enter into interinstitutional negotiations in October 2017.

The Council adopted its general approach in June 2017. In particular, it aimed to exclude from the scope of the regulation the processing of 'operational personal data', such as data processed for criminal investigations by EU bodies such as Eurojust and Europol (at least when the establishing acts of these bodies provide for data protection rules, with the latter prevailing over the revised regulation).

Trilogue negotiations on the file advanced under the Estonian and the Bulgarian Presidencies. The main issue at stake was the scope of the regulation and thus setting specific requirements for operational data of the EU's justice and home affairs agencies while keeping a harmonised framework. The European Parliament rapporteur insisted on including EU agencies dealing with data processing in the area of law enforcement (Eurojust, Europol and EPPO as well as missions) within the scope of application of the new rules, and suggested introducing an additional chapter on operational data (*Chapter VIII-a*) within the same regulation. Specific provisions of the founding acts of these agencies would only give details and complement the revised Regulation 45/2001. The Council, by contrast, was leaning more towards excluding these EU agencies from the scope of the new regulation.

A compromise was reached two days before 25 May 2018 (the date originally planned for its adoption, in parallel with GDPR); the delay in the adoption of the new rules may potentially create discrepancies, at least for the time being, between the level of protection offered by the general rules of GDPR and that offered by the current Regulation 45/2001. The political agreement is, however, a meaningful sign of a common will to build a coherent data protection framework.

General principles and requirements

Scope

The new regulation will apply to data processing by automated means or otherwise, if part of a filing system by Union institutions and bodies, including the transfer of data between them or to other recipients established in the Union.[12]

According to the compromise text (Article 2), this regulation will not apply to the processing of operational personal data by Europol and the European Public Prosecutor's Office, until the respective acts (Regulations No 2016/794 and No 2017/1939) are adapted, nor to missions. A new Chapter VIIIa has been included (as requested by the Parliament, but modified in the compromise text) with general rules on processing of *operational personal data* by Union agencies, offices and bodies when carrying out activities in the field of judicial cooperation in criminal matters and police cooperation: specific provisions in the founding acts of the agencies are maintained.

Own definitions

Article 3 of the compromise text includes both definitions specific to this regulation, e.g. that of 'Union institution', 'controller', 'user', 'operational personal data' or 'directory',[13] and definitions that are identical to the GDPR (e.g. that of consent, processing, profiling, etc.).

Regarding its own definition of data **controller**, unlike the GDPR, the proposal does not include in its definition the reference to *natural* persons. Therefore, according to *new* Regulation 45/2001 a controller is: a Union institution, body, office or agency, or a directorate-general or *any other organisational entity* (this could potentially also include parliamentary groups or the office of an

MEP) that determines, also jointly, *the purposes and means* of data processing; also 'controllers *other than* Union institutions and bodies' means controllers within the meaning of Article 4(7) GDPR, which considers as a controller *any natural or legal person, public authority*, or other body determining the purposes and means of personal data processing. The new definition does not include *'unit'* (this term is used in current Regulation 45/2001), but it may be included if considered as an 'organisational entity'. Each controller shall maintain a **record** of processing activities under its responsibility. The data processor, is, rather, defined as 'the natural or legal person or public body processing data on behalf of the controller'.

Main principles and rules

Changes introduced with the reform include increased transparency and confidentiality requirements, in line with the GDPR. Personal data must be collected for specified, explicit and legitimate purposes and not further processed in an incompatible way (Article 4). More flexibility is provided than in the GDPR, with conditions, as regards data processing for **other compatible purposes** (than that for which data were initially collected).[14]

The criteria for lawful data processing replicate those of the GDPR (consent, necessity to perform a task *in the public interest or in the exercise of official authority vested in the Union body*, or in compliance with a *legal obligation*, etc.) with the exception of the controller's legitimate interest, which is not applicable to the Union institutions (Article 5).[15] In line with the GDPR, **consent**, to be valid as legal grounds, must be freely given and unambiguous, expressed by a clear affirmative act (including ticking a box); silence, pre-ticked boxes or inactivity should not constitute consent; on the other hand, consent could cover all processing activities carried out for the *same* purposes. Therefore, processing data for the same purposes for which the institution, as controller, has got already the subject's consent does not require new consent, as far as the controller can demonstrate that a clear indication of consent was obtained in the past. However, information obligations apply.

Also, according to the principle of **accountability**,[16] the data controller needs to be able to *demonstrate* compliance with the regulation.[17] It is clear that the designation of a data controller within the EU institutions implies a series of obligations and tasks (Chapter IV of the new regulation).

Regarding special categories of data, (e.g. on health, or religious or political persuasion), derogations from the general prohibition to process them (Article 10) include: processing carried out in the course of its legitimate activities by a non-profit-making body which constitutes an *entity integrated in a Union institution* or body and with *a political*, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; another derogation applies if processing relates to data that are manifestly made *public* by the data subject.

With a view to strengthening individuals' **rights**, the proposal places obligations on data controllers, such as to provide transparent, easily accessible **information** (save derogations) as well as mechanisms for exercising their rights (including electronic requests). Information must include the storage period, the right to lodge a complaint and possible international transfers; an **exception** applies if personal data must remain subject to an obligation of professional secrecy regulated by EU law (e.g. data processed by services competent for social security or health matters).

Moreover, the subject's rights include the *right to access* (his or her data being processed by the institutions), the right to erasure (*'right to be forgotten'*), as well as the right to restrict processing in certain cases (former 'right to blocking') from the controller, the right to *data portability* (to transmit data to another controller), and the *'right to object'* to certain forms of data processing.

According to the compromise text on the proposal, restrictions to these rights – which are necessary and proportionate to safeguard national security, public security, the prevention, investigation of crimes, the internal security of the institutions or another important *general public interest* of the Union or of a Member State, like common foreign and security policy, and which uphold the *essence*

of fundamental rights[18] – may be adopted by a legal act on the basis of the Treaties or **by the internal rules** of Union institutions in matters relating to the *operation* of the institutions.[19] The indication of internal rules as grounds for restricting data protection rights was among the political issues raised during the trilogues.

The text resulting from the trilogues (Article 25) seems designed to allow for EU institutions' internal rules as a basis for restrictions of rights, but (in compliance with Article 52(1) CFR) providing they are *clear and* ***precise acts of general application***, intended to produce legal effects vis-à-vis data subjects, adopted at the *highest level of management* of the institutions and subject *to publication* in the Official Journal (acts such as internal guidelines of an institution seem to be excluded).

Another novelty, in line with the GDPR, is the right of the subject to object to data processing, although necessary for a task carried out in the public interest (including profiling), and not to be subject to a *solely* automated decision (i.e. a decision affecting an individual based solely on automated processing, without human intervention), for instance for e-recruitment. Also, the principles of **data protection by design** (where the data processing system is designed from the outset to minimise the collection of data by means, for instance, of pseudonymisation) and **by default** (only necessary data should be processed), are now extended to the Union institutions.

Enforcement and control

A data protection **impact assessment** will be conducted by a controller prior to data processing operations that might result in high risks to the rights of individuals (e.g. if using new technologies to evaluate personal details of persons based on profiling). If data processing results in high risks consultation with the EDPS is mandatory.

Regarding the **DPO**, his or her position is also strengthened and the EU institutions must ensure that he or she is involved in all issues that relate to the protection of personal data. The DPO's tasks will include: informing and advising the controller; ensuring in an independent manner the internal application of the regulation and monitoring compliance with it and other data protection policies.

As the current Regulation 45/2001 defines the powers and duties of the **EDPS**, the new proposal contains several provisions aimed at strengthening these powers.[20] While the new regulation confirms, inter alia, the EDPS's task of **monitoring and enforcing** the application of this regulation by a Union institution or body, with the (only explicit) exception of the processing of data by the CJEU acting in its judicial capacity, it also clarifies the EDPS's investigative powers (Article 59).[21]

When it comes to the regime of **remedies**, the proposal confirms the right of any data subject to lodge a complaint with the EDPS and the right to compensation for both material and non-material damage. Tougher **sanctions** are provided in cases of infringement, and the EDPS has the power to impose **administrative fines** on Union institutions and bodies where the controller/institution failed to comply with an *order* of the EDPS.

Attention is paid also to the confidentiality of electronic communications to be secured by the Union institutions, in particular by securing their electronic communication networks (new Section 2a). The draft regulation also protects data relating to the terminal equipment of end-users accessing publicly available websites and mobile applications offered by Union institutions, in accordance with the current e-Privacy Directive and in view of the upcoming e-Privacy Regulation.

The EDPS adopted **practical guidelines** in early 2018 to help EU institutions processing personal data,[22] taking into account the GDPR. In particular, the guidelines provide recommendations on implementing accountability for data protection by outlining the approach the institutions should take in the development and maintenance of the information systems and databases (including 'privacy by design') as well as when opting to process data using cloud-based services.[23]

GDPR or Regulation 45/2001? Or are MEPs in a class of their own?

As mentioned above, a special regime exists for data processing by EU institutions and bodies (current Regulation 45/2001). The GDPR explicitly rules out its applicability to this kind of processing in Article 3. The new Regulation 45/2001 will apply to processing of personal data as regards parliamentary activities, at least unless stated otherwise.

The issue that may emerge as regards the applicability of data protection rules to individual MEPs[24] (whether to apply just Regulation 45/2001 and its update, the GDPR, or both)[25] might require prior clarification of whether MEPs should be considered at all times in their quality as part of the European Parliament (and therefore as falling under the rules for EU institutions) or not: it seems that the prevailing interpretation is to consider MEPs, whether taken in parliamentary groups or individually in their capacity of Member, and processing personal data in the **exercise of their European mandate**, as forming European entities, and thus **subject to Regulation 45/2001** and its update:[26] Data processing activities should be considered as one of the responsibilities of the MEP, and, in case, involving the Parliament (or an entity inside it) as data processor or co-controller.[27]

Also, it should be stressed that owing to the variety of tasks and areas covered by the Parliament, data protection requirements must be determined on a case-by-case basis. The application of the GDPR could for instance be envisaged in any case where an MEP acted as an ordinary citizen or as a national parliamentarian and not in the exercise of his/her function as European parliamentarian. In any case, whichever regulation is applicable, the main substantial principles and values underlying their rules are equivalent and pursue the same objectives.

The following situations and potential applicability of data protection rules could be considered:

1 MEPs as *data subjects* (of data-processing by EU institutions) – current or new *Regulation 45/2001*
2 MEPs in the exercise of their functions – *current or new Regulation 45/2001*
3 MEPs when not acting as MEPs - GDPR and national data protection laws

Still, it may be advisable for the law- and policy-makers to better clarify whether MEPs can be considered as *sui generis* data controllers in light of the new Regulation 45/2001 (and therefore subject to the related obligations) or not. More importantly, it would be worth clarifying to what extent the political role exercised implies a sort of 'inapplicability in practice' of the supervisory system of data protection (e.g. MEPs acting in their capacity would not be subject to oversight as other data controllers and European Parliament staff). The reasons may be found in their political mandate, as representatives of Union citizens, and in the need to provide specific rules for them in order to guarantee them the freedom to exercise their functions: the European Parliament, according to the Treaty on European Union (Article 14), exercises the functions of *political control*. As also indicated in the Rules of Procedure and the Statute for Members,[28] MEPs shall exercise their *mandate freely and independently*.[29] While MEPs are bound by data protection rules for EU institutions and any infringement would still be an unlawful act, in principle supervision mechanisms (such as audits) might be restricted to the extent that there is a strict link between data processing and the exercise of their mandate (similar to the immunities regime as interpreted by the CJEU).[30] However, it remains to be clarified whether or not, and to what extent, the *supervision* mechanisms provided by Regulation 45/2001 (and its update) could be limited with regard to individual MEPs, but with the rest of the regulation's provisions applicable. Data processing within the European Parliament's administration is in any case subject to Regulation 45/2001: so the EP is the controller of the data-processing operations concerning the recruitment procedure for assistants and access control to EP premises for visitors.

The 2005 Bureau decision, implementing Regulation 45/2001, mainly describes the powers and duties of the DPO appointed in the European Parliament and the data subjects' rights (e.g. request to access to data).[31] No mention is made of the DPO's role (if any) in relation to the data processing carried out by individual MEPs,[32] nor of whether the latter can be considered data controllers or not. The only activity that seem to be taken into account is the data processing carried out by the EP's staff.[33] As regards the monitoring procedure, the DPO may carry out any type of monitoring at any time in order to ensure the application of Regulation 45/2001

by the European Parliament; the DPO should cover all the data processing operations performed by the EP, its Members and the political groups. One DPO could work for all, or a number of, MEPs.

The issue of data processing by individual MEPs, and in particular of the control and supervision (by the internal DPO and by the EDPS) of their activities might be clarified hopefully before the adoption of the new regulation (and in collaboration with the EDPS). Similar open issues might be posed as regards the activities of the **Parliament's political groups**, into which MEPs can organise themselves, entailing data processing (the European political parties meanwhile are treated differently and should be covered by the GDPR and national laws as mentioned above). Given the role of the DPO in ensuring the application of the new rules within the European Parliament, a single DPO for all parliamentary groups might be a possibility (in any case, different from the DPO responsible for the EP administration).

Further considerations

As a suggestion, further clarification of the application of new Regulation 45/2001 to MEPs (and to political groups) could be contained in an act of the Parliament, such as a Bureau decision. However, if this is contained in internal rules and restricts individuals' rights, it should respect the conditions established in the new Article 25 (i.e. they should be precise acts of general application, adopted at the highest level of management of the institution and published in the Official Journal).

With regard to the independent authority that, according to Article 16 TFEU, should monitor compliance with data protection rules, this, as regards MEPs should be the EDPS.

It should be stressed that, in any case, substantial data protection principles (contained for instance in the CFR, the ECHR and CoE Convention 108) should be observed.

Outlook

This briefing seeks to provide an overview and some cues for discussion of the main data protection principles and rules applicable to Parliament and its Members. It is based on the current and upcoming legal framework as well as on current practice. It also highlights a number of critical issues and suggests that the upcoming reform in the field may provide the opportunity to discuss and possibly clarify these issues. An update of this briefing is envisaged alongside the adoption of the proposed new regulation that will replace Regulation 45/2001.

MAIN REFERENCES

Protection of individuals with regard to the processing of personal data by the EU institutions, bodies, offices and agencies and the free movement of such data, European Parliament, Legislative Observatory (OEIL).

EDPS, New data protection rules for the EU institutions, press release, 23 May 2018.

Article 29 Working Party, Statement on the review of Regulation 45/2001, April 2017.

Monteleone S., Rules for EU institutions' processing of personal data, EPRS, European Parliament, April 2018.

Monteleone S., GDPR goes live: A modern data protection law EPRS, European Parliament, May 2018.

Assessment of the impact of specific aspects of the new model of governance and accountability of data protection by Union institutions and bodies proposed by the Commission, substitute impact assessment, EPRS, European Parliament, October 2017.

ENDNOTES

[1] Article 16 TFEU recognises the right to data protection for any individual, and provides that the rules adopted by the EU and Member States acting within the scope of EU law and related to data protection are to be laid down following the ordinary legislative procedure and that compliance with these rules shall be subject to the control of independent authorities. At the level of international treaties, mention should be made of Article 17 of the ICCPR, Article 8 of the ECHR (on the right to privacy) and Council of Europe Convention 108/1981, the first international legally binding instrument on the automatic processing of personal data (see its recent amending protocol).

[2] European Commission proposal for a regulation on data protection in the EU institutions, explanatory memorandum.

[3] New Regulation 45/2001 also requires EU bodies to comply with e-Privacy rules. An e-Privacy Regulation is also under way, although delays in the legislative process prevented the presentation of a complete framework by 25 May 2018.

[4] See Case T-82/09, *Dennekamp v Parliament*, on the (upheld) refusal by the EP to grant the applicant access to documents regarding the affiliation of certain MEPs to the additional pension scheme, for reasons of data protection.

[5] The EDPS has the power: to give advice to data subjects on their rights; to warn or admonish the controller; to order the rectification or erasure of data processed in breach of the law; to impose a temporary or definitive ban on processing; to obtain access to any premises in which 'a controller or Community institution or body carries on its activities when there are reasonable grounds for presuming that an activity covered by this regulation is being carried out there' (Article 47.2).

[6] See for instance the Privacy Statement released by the EP on the occasion of an interparliamentary committee meeting.

[7] See Case F-46/09 *V. & EDPS v. European Parliament* in which the EU civil service Tribunal annulled the decision of the European Parliament to withdraw the offer of employment to the plaintiff because in breach of Regulation 45/2001.

[8] See for instance the Guide for users prepared by the EP on the basis of Regulation 45/2001 and the website legal notice.

[9] See also Article 14 of the 2015 EP Bureau Decision on monitoring procedure: the DPO may decide to carry out any type of monitoring at any time in order to ensure that the Regulation [45/2001] is properly applied by the European Parliament.

[10] Accordingly (Article 86), any failure by an *official* to comply with his obligations under these Staff Regulations, whether intentionally or through negligence on his part, shall make him liable to disciplinary action. Where the appointing authority or OLAF becomes aware of evidence of failure within the meaning of paragraph 1, they may launch administrative investigations to verify whether such failure has occurred.

[11] The text in the square brackets is present in the proposal, but disappeared in the compromise (Article 1).

[12] As in the previous note; it has been also deleted the reference 'insofar as such processing is carried out in the exercise of activities which fall within the scope of Union law' (Article 2).

[13] Article 3.2.d defines 'directory' as a publicly available directory of users or an internal directory of users available within a Union institution or body or shared between Union institutions and bodies, whether in printed or electronic form.

[14] Further processing for archiving purposes in the public interest, scientific, research or statistical purposes shall not be considered to be incompatible with the initial purposes (Article 4).

[15] However, see Article 23 of the proposal, where compelling legitimate grounds of the institution, over-riding individuals' rights, once demonstrated, can restrict the right to *object* of Article 23.

[16] In line with the principle of accountability of the GDPR, the controller shall demonstrate that the subject has consented to the processing of his or her data; when assessing if the consent is freely given, it should be taken into account whether the performance of a contract, including the provision of a service, is conditional on consent to data processing that is not necessary for the performance of that contract. See, inter alia, EDPS provisional guidance on accountability.

[17] This includes the adoption of appropriate technical and organisational measures and, where appropriate, *internal policies* and mechanisms for ensuring such compliance. See also the report published in 2017 by the EDPS, which will support the EU institutions in moving towards an accountability-based approach.

[18] On the problematic definition of this concept see, inter alia, M. Brkan, In Search of the Concept of Essence of EU Fundamental Rights through the Prism of Data Privacy Maastricht Faculty of Law Working Paper, No 2017-01.

[19] The reference contained in the original proposal that 'Even in the absence of a legal act or internal rules, an EU institution may restrict these rights in relation to a specific processing operation' has been deleted in the compromise.

[20] The proposal will also repeal Decision No 1247/2002/EC governing the EDPS's duties.

[21] These include: to carry out investigations in the form of data protection audits; to obtain, from the controller access to all personal data and information necessary for its tasks; to obtain access to *any premises of the controller*, including to any data processing equipment and means, in accordance with Union law.

[22] See Action 8, 'Continue to support EU institutions in moving beyond a purely compliance-based approach to one that is also based on accountability'. See also, the International data protection commissioners' conference to be held in Brussels, in October 2018.

[23] Moreover, the EDPS published provisional guidance on transparency rights and obligations according to the proposed regulation and guidelines on accountability in documenting processing operations.

[24] See on a different issue J. Kunert, 'Members of the European Parliament on the Web', 2015, where they are defined as distinctive parliamentarians, because they are members of the European Parliament, a special political environment.

[25] See similar issues discussed, at national level, in the recent study by the German *Bundestag*'s research service.

[26] See Article 29 Working Party, Opinion on the concept of controller and of processor, 16 February 2010, footnote 13.

[27] The European Parliament, for instance, supplies MEPs with technical support, including IT systems, facilities, maintenance, and security.

[28] See in particular, Article 2 (Members shall be free and independent); also Article 4 states that 'Documents and electronic records which a Member has received, drafted or sent shall not be treated as Parliament documents unless they have been tabled in accordance with the Rules of Procedure'. The rationale behind this provision seems to be to avoid these documents being subject to the regime for access to European Parliament documents and to protect their confidentiality.

[29] On the other hand, there are indications of the need to respect data protection also in parliamentary activities that are directly related to the Members' *mandate* in some provisions of secondary law. For instance the right to inspect files, provided for by Article 6 of the Statute for Members and in the Rules of Procedure, as 'essential for the exercise of the Members' mandate' finds its limitation precisely in 'personal files and accounts', thus in data protection rights.

[30] For instance, according to Rule 2, Members shall exercise their mandate freely and independently, shall not be bound by any instructions and shall not receive a binding mandate. Rule 5 states that Members enjoy the privileges and immunities laid down in the Protocol No 7 on the Privileges and Immunities of the EU (see for example Articles 7, 8 and 9). Parliamentary immunity is not a Member's personal privilege but a guarantee of the independence of Parliament as a whole. On the functional link between an MEP's activity and the exercise of the mandate, necessary for the application of the immunities regime, see the *Patriciello* case (C-163/10).

[31] See Article 2: the DPO shall be independent in the performance of his/her duties; he/she may not receive any instructions, in particular from the appointing authority, the Secretary-General or any other source. Article 7: the register (kept by the DPO) shall detail the notified processing operations carried out at the European Parliament and indicate the department responsible for the processing and the purpose.

[32] In Article 6 on the obligation on the data controller to provide the DPO with information includes the name of the latter and the European Parliament departments that are entrusted with the data processing for a particular purpose.

[33] Article 17 of Decision states that the Secretary-General may appoint an authority subordinate to h/her as a data controller according to Art 2 Reg. 45/2001, responsible for, inter alia, giving the members of the European Parliament's *staff* (or other persons under their authority) suitable instructions for ensuring that processing is confidential (however, a data controller, as responsible of data processing should in any case be identified to comply with Regulation 45/2001).

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)