Local Staff Committees The Hague, Berlin & Munich
Central Staff Committee

Munich/The Hague, 12.02.2019
sc19004 – 0.2.1/1.3.1

Data protection@EPO
Quo vadis?

Summary: New regulations for data protection entered into force in the EU in 2018. Staff representation finds that this is an opportunity to re-open the discussion on data protection at the EPO: The data protection policies at the EPO should be improved in order to better protect the data of staff and users alike. They do not reach by far the standards of the new EU regulations, which is an inacceptable situation when processing applications from EU member states. The EPO used to have a long tradition to strive to comply with the highest standards in data protection. The last reform in 2014 can only be seen as deterioration in this matter. An alignment of the data protection guidelines of the EPO to EU regulations would be a step towards a modern data protection framework and would contribute to establish the EPO as the leading patent office.

We suggest that:

- *The EPO policies on data protection should be aligned to the EU regulations, which present at the moment the most comprehensive and modern legislation in data protection matters.*
- *The role of the Data Protection Officer, who is responsible for the implementation of the EPO data protection, should be enforced and its independence should be assured.*
- *An external and independent oversight body should be appointed with the task to monitoring the application of data protection policies at the EP.*
- *Separate data protection policies should be defined for investigative procedures (e.g., misconduct or fraud). Its supervision should be the responsibility of a distinct Data Protection Officer nominated, e.g., by the Administrative Council.*
- *Rules to safeguard data processing should be introduced. For example, transfer of personal data to third countries and the change of purpose, e.g., using personal data for purposes for which the user has not unequivocally consented to, should be tightly regulated.*

Figure 1: As of May 2018, with the entry into application of the General Data Protection Regulation (GDPR)[1], there is one set of data protection rules for all companies operating in the EU.

The GDPR: a new EU regulation on data protection

On 25.5.2018 a new European regulation on data protection has entered into application, the General Data Protection Regulation[1] (GDPR). It safeguards EU citizens' fundamental right to protection of their data and it is binding for all EU member states. The GDPR brings several improvements[2]:

Clear language: Privacy policies will have to be written in a clear language.

Consent from user: The user will need to give an affirmative consent before his/her data can be used by a business. Silence is no consent.

More Transparency: Businesses will need to inform the user when his/her data is transferred outside the EU. They will be able to collect and process data only for a well-defined purpose and will have to inform the user about new purposes.

Stronger rights: Businesses will have to inform users in case of data breach. The user will have the right to access and get a copy of the data a business has on him.

Strong supervision: Newly introduced independent Supervisory Authorities monitor the implementation of the regulations.

EU regulations not binding for EPO

The EPO does not belong to the European Union, hence the GDPR is not binding for the EPO[3,4]. The EPO follows its own data protection policies: the Data Protection Guidelines[5] (DPG). The DPG were unilaterally adopted by the President and entered into force in 2014.

[1] 2018 reform of EU data protection rules, link, text of law, link
[2] A new era for data protection in the EU, What changes after May 2018, link , On Wikipedia, link
[3] See section 9 "Data protection framework", Breaches of basic and fundamental rights at the EPO, Bretton Woods Law, Legal Opinion, 2016, link
[4] The fact that the EPO does not honour the GDPR can easily be diagnosed opening the Internet sites of the DPMA (Deutsches Patent- und Markenamt) and the EPO: only on the DPMA site does a request for acceptance of cookies open. Furthermore, the EPO site is not transparent about its data protection policy.
[5] Guidelines for the protection of personal data in the European Patent Office, link

EPO data protection guidelines are insufficient

An independent and external legal analysis[3] in 2016 concluded that the DPG didn't meet the standards of data protection laws in the EU at that time. The analysis further stated that there is a lack of independent oversight, of an effective system of checks and balances to prevent abuses[6], and of effective means of redress in circumstances where the rights of individuals are infringed.

Staff representation proposes to align EPO policies to EU policies

Staff representation continuously voiced critique[7,8,9] on the DPG[10], and sees the wide public discussion leading to and the introduction of the new European regulation as an opportunity to open a new discussion on data protection at the EPO. A gap analysis[11] conducted by the Staff Committees The Hague and Munich reveals significant differences between EPO and the new EU regulations. With this paper we would like to encourage the administration to take action. We believe that the data protection guidelines at the EPO are insufficient and especially with the introduction of the GDPR they should be revised and updated. We list five major points below.

Data protection and the Unitary Patent

One argument for a timely alignment of the DPG with the GDPR is the possible introduction of the Unitary Patent. The EPO would be entrusted by the EU to process the Unitary Patents and would then act comparable to a European agency. It is unlikely that member states and applicants would accept a situation in which the EPO would process personal data of EU citizens in the name of the European Union without respecting EU legislation for data protection.

1 One system is better than two: Alignment of the EPO regulations to the EU regulations

We regard the GDPR as the most modern and up-to-date regulation about data protection. In order to continue the tradition the EPO once had to strive to comply with the highest standards in data protection matters[12] we argue that an alignment of its data protection guidelines with EU regulations is necessary. EPO applicants and EPO staff alike deserve the

[6] For example, under the DPG, no role is foreseen for the Staff Committee. All references to the Staff Committee contained in previous versions have been deleted.
[7] Appendix 1: Report on data protection, Letter to AC, Central Staff Committee, 25.02.2016, link
[8] History of DPG@EPO, Staff Committee The Hague, 25.5.2018, link
[9] GAC/AV 4/2014, Opinion of the CSC about Data Protection Guidelines, link
[10] Communication VP5, EPO intranet, 25.5.2018, link
[11] Gap Analysis of DPG and GDPR, Staff Committee The Hague, 2018, link
[12] Data protection – Current situation in the EPO and in Europe, Gazette 15/95, 03.07.1995, page 8, link

best standards: data protection is one major quality feature of an organisation. Although a number of features and wordings are similar to the EU regulations, the DPG are not in conformity with them, and would not be adequate for any EU institution or private company.

Aligning the DPG with the GDPR would also solve many practical problems with regard to personal data handling at the EPO. Due to its territorial scope the GDPR[13] will sometimes apply for personal data processed by the EPO. For example personal data regarding external contractors or applicants will fall under the GDPR while internal personal data might not. In some cases it will be difficult to clearly define which regulation applies, the EPO guidelines or the EU guidelines. This situation would naturally be solved by bringing the DPG in line with the GDPR.

2 Reinforcing the Data Protection Officer

At the EPO the implementation of the DPG are supervised by the Data Protection Officer. According to the DPG the Data Protection Officer should be independent and have adequate resources[14].

Since the reform of the DPG in 2014 staff representation criticized the implementation of the rules regarding the Data Protection Officer: There are little institutional guaranties for the independence of the Data Protection Officer. He is selected and appointed for two years by the President alone and stands in direct line of hierarchy under him. Besides his function as Data Protection Officer he also holds other functions at the EPO (e.g., director), which effectively compromises his independence and impartiality. The situation before 2014 was slightly better, as the Data Protection Officer was appointed after consultation of staff representation. Such consultation also ensured that the data protection officer would be designated on the basis of professional qualities, in particular expert knowledge in data protection[15].

3 Appointment of an external oversight body

A key component of the GDPR is the introduction of independent and public oversight bodies, the Supervisory Authorities[16], which monitor the correct application of the policies regarding data protection in the member states. It also receives complaints concerning breaches of the guidelines. For EU institutions, such as the European Parliament, these tasks are carried out by the European Data Protection Supervisor[17].

[13] as defined in Art. 3 of the GDPR (territorial scope), link
[14] Art. 18 DPG: i.e. sufficient staff and financial resources, link.
[15] Art. 37(5) GDPR
[16] Art. 51 GDPR, Supervisory authority, link
[17] European data protection supervisor, The EU's independent data protection authority, link, GDPR, Articles 51-56

The EPO does not have such an external and independent oversight body. The oversight body cannot be located under the direct supervision of the President because of its need for impartiality and independence. It might be conceivable to introduce such an independent body within the Administrative Council, thereby mirroring the EU model. However, it would be challenging to vest it with the necessary competence. Another possibility appears to be the recognition of the European Data Protection Supervisor as the competent supervisory instance for the EPO.

4 Definition of separate data protection policies in the context of investigative procedures

The DPG explicitly excludes its application for internal investigative procedures[18]. Accordingly, the Data Protection Officer is bypassed in such procedures. Internal investigative procedures are carried out by directorate Ethics and Compliance[19] in order to investigate facts related to potential misconduct of EPO staff, e.g., in cases of fraud.

In general, investigative procedures are subject to less strict regulations in order to facilitate detection of crimes. However, on a national level there exists a real separation of power, by which each investigative body acts independently, and has distinctive Data Protection Officers assigned in conformity with national regulations. Certain investigation procedures requiring access to personal data can even be dependent on the confirmation of an independent judge.

At the EPO the President ultimately is in charge of defining all data protection policies. This introduces an obvious conflict of interests. In practice the director of directorate Ethics and Compliance decides alone on proportionality of data collection and processing regarding investigative procedures[20]. However, he is in direct line of hierarchy under the President and finds himself in a conflict of interests. There are no independent institutional checks and balances.

In a publicly known example[21], surveillance and tracking software has been installed on a computer in a public area of the EPO, on which sensitive data of applicants, representatives and members of the AC could have been processed. It is not clear who authorised this and how the Data Protection Officer was involved.

[18] In the new Investigation Guidelines introduced by CA/D 7/17 (link) all references to any data protection guidelines or data protection officer have been removed.
[19] Department, 0.6.4 Ethics and Compliance, link
[20] See Art. 16(3) Implementing Rules for Articles 21, 21a and 93 Paragraph 2 ServRegs
[21] "Spy scandal – EPO hits the news in Germany", ipkitten, 09.06.2015, link

One possible way to overcome this severe deficit of independent control of data protection for investigative procedures is the nomination of a distinct Data Protection Officer by the Administrative Council, this Data Protection Officer possibly even belonging to the administration of the Administrative Council. The framework of appointment of the chairpersons of the internal appeals committee could be used as a model.

5 Safeguarding purpose and transfer of personal data

The GDPR sets out high standards for keeping the purpose and transferring personal data to third countries. For example, a change of purpose is not allowed without the explicit consent of the user: it would not be allowed to use address data which has been collected to invoices for sending advertisement. Furthermore, businesses will need to inform the user when his/her data is transferred outside the EU for processing.

At the EPO the President has the power to decide on any matter concerning the change of purpose[22] and transmission of personal data outside the EU or the member states of the European Patent Organisation[23]. A formal consultation of the Data Protection Officer is necessary but the President is not required to follow his opinion. Staff representation or independent supervisors are not involved at any stage.

Also for the transfer of personal data to third countries, it is the President who decides if the level of data protection of personal data in that country is to be considered as adequate. The GDPR on the other hand sets out strict requirements[24], e.g., the rule of law and the respect of human rights in that third country. We do not see any reason why these requirements should not be respected also by the EPO.

Conclusions

The data protection guidelines at the EPO should be revised with the objective to align them to the new EU regulations which represent the new golden standard in data protection. Competent bodies of the EU, external consultants and staff representation should be involved in this process. The EPO used to have a long tradition to comply with the highest standards in data protection matters[25]. The last reform in 2014 can only be seen as deterioration in this matter[9]. An alignment of its data protection guidelines to EU regulations would contribute to establish the EPO as the leading patent office.

[22] see Art. 6 (1) and 12 (1) DPG, link
[23] see Art. 8 DPG, link
[24] GDPR, Article 46, link
[25] Data protection – Current situation in the EPO and in Europe, Gazette 15/95, 03.07.1995, page 8, link