TaylorWessing

GDPR Processor Obligations

While former data protection laws, such as the European Data Protection Directive 95/46/EC (the "Directive"), mostly addressed data controllers, the General Data Protection Regulation ("GDPR") imposes several obligations upon data processors. Before its entry into force in 2018, the controller was entrusted with ensuring compliance when employing processors via contractual agreements; the GDPR's approach is different: Although processors are still bound by the controllers' instructions, the GDPR allocates responsibilities between the parties by assigning processors an active role and introducing direct statutory obligations as well as significant fines of up to 4% of the global annual turnover of the processors.

Companies acting as data processors within the scope of the GDPR, should assess their legal role and ascertain that they have implemented GDPR standards.

1 Technical and organizational requirements

The GDPR stipulates several requirements regarding a processor's organization, such as:

Representative in the EU, Art. 27 GDPR

Processors subject to the GDPR but without establishment in the EU must appoint a representative, just as controllers are obliged to.

Implementation of Technical and Organizational Security Measures, Art. 28 Sec. 1, 3, Art. 32 GDPR

The Directive relied on the controller to contractually require the processor to secure the personal data processed on its behalf. The GDPR obliges every processor to implement appropriate and reasonable state of the art technical and organizational measures. Processors therefore have to comply with the same security requirements as controllers, including

- Pseudonymisation and encryption
- Ensuring the confidentiality, integrity, availability and resilience of processing systems and services
- The ability to recover and restore the access to lost data
- Regular evaluation of the technical and organizational measures taken

Support of the controller in conducting Data Protection Impact Assessments, Art. 28 Sec. 3 phrase 1 lit. f, 35 GDPR

Where a data processing activity is likely to result in a high risk to the rights and freedoms of natural persons, controllers shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations (Art. 35 GDPR). Processors are not obliged to conduct Data Protection Impact Assessments themselves but have to support the controller in doing so.

Records of processing activities, Art. 30 GDPR

Under the GDPR, most processors have to increase their accountability activities by maintaining records of their data processing activities, which must be made available to supervisory authorities on request. While similar to the records kept by controllers, they are less comprehensive, containing in particular the following information:

- Name and contact details of the processor, the controller(s) it works for and its data protection officer
- The categories of processing carried out
- Transfers of personal data to a third country and the documentation of the suitablesafeguards
- A general description of the technical and organizational security measures

Data Breach Notifications, Art. 33 Sec. 2 GDPR

Processors have to notify the controller on behalf of which they are processing data without undue delay after becoming aware of a personal data breach (any accidental or unlawful destruction, loss, alteration, unauthorizsed disclosure of, or access to, personal data). Often, more specific timelines will be specified in the contract between the controller and the processor.

Data Protection Officer, Art. 37 GDPR

Processors under the GDPR have to designate an independent, reliable and knowledgeable data protection officer under the same conditions as controllers, meaning they are obliged to do so if their core activities consist of

- Processing which requires regular and systematic monitoring of data subjects on a large scale
- Processing on a large scale of special categories of data (e.g. health, religion, race, sexual orientation etc.) and personal data relating to criminal convictions and offences

A group of undertakings may appoint a single data protection officer provided that such data protection officer is easily accessible from each establishment. Thus, one global data protection officer steering data protection EU-wide may prove helpful in order to cope with differing EU-wide regulations. Please note that national laws may require the implementation of data protection officers in additional cases (which is e.g. the case in Germany).

Notification regarding the infringement of data protection obligations

If a processor believes a controller's instruction infringes data protection obligations, it must inform the controller immediately (Art. 28 Sec. 3 phrase 2 lit. h GDPR). However, the processor is not obliged to verify the material lawfulness of the obligation, but only needs to inform the controller if doubts arise during its processing activities.

Safeguards for third country data transfers, Art. 44 GDPR

Whereas the Directive emphasized the controller's obligation to ensure the lawfulness of third country data transfers, the GDPR places the obligation to create sufficient safeguards for such transfers on both the controller and the processor (Art. 44 GDPR). Therefore, processors must ensure that any data transfer outside the EEA is covered by sufficient safeguards under Art. 44 et seq. GDPR (such as Standard Contractual Clauses, EU-U.S. Privacy Shield certification, etc.).

2 Direct interaction of processors with supervisory authorities and data subjects

The GDPR stipulates several requirements regarding a processor's organization, such as:

- Processors under the GDPR are obliged to cooperate directly with supervisory authorities upon request (Art. 31 GDPR), while the Directive mostly limited supervisory contacts to controllers.
- Data subjects under the GDPR are entitled to enforce damage claims against processors. A processor is liable for damages caused by processing if it has acted contrary to its legal obligations or lawful instructions of the controller (Art. 82 GDPR).
- Data subjects cannot exercise their rights to information, access etc. (Art. 12-23 GDPR) towards processors. However, the processor must support the controller for whom he is processing in responding to data subjects' requests.

3 Detailed data processing agreement

Under the Directive, data processing agreements between controllers and processors have been mandatory, but the contract often included only very basic obligations. Under the GDPR, the relationship between controller and processor needs to be regulated in detail (see Art. 28 GDPR), including with respect to the following obligations of the processor:

- To generally process the personal data only on documented instructions of the controller
- To ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- To secure the processing by appropriate technical and organizational measures
- To comply with stricter sub-processing rules (the sub-processing contract needs to reflect the requirements of the data processing contract between the controller and the processor, and prior written approval of sub-processors by the controller will be required, although a general and abstract approval of sub-processors will remain permissible as long as the controller is allowed to object to the appointment of specific sub-processors)
- To assist the controller with appropriate technical and organizational measures in responding to data subjects' requests
- To assist the controller in compliance with the latter's obligations regarding security of processing, data breaches and Data Protection Impact Assessments
- To return or delete all personal data after the end of services unless obliged to retain the data by law
- To make available to the controller all information necessary to demonstrate compliance with the latter's obligations regarding processing by a processor and allow for and contribute to audits, including inspections

Annex

Guidance on the definition of "processor" and "controller" under the GDPR

Within the scope of the GDPR, the concept of processor and controller is crucial as the GDPR attaches different responsibilities and obligations to each role. This being said, in order to determine whether you are a processor or controller, a case-by-case analysis is required as this is always a question of fact. The following provides guidance plus a bundle of indicators and examples for the individual assessment. Please note that the following summary cannot be exhaustive and only intends to illustrate the basic criteria for the distinction of both roles. In case of doubt, please contact your data protection officer or legal department.

Remark: Please note that usually it is preferable that you transfer personal data only to processors. The reason being that controllership ensures that personal data is only processed according to your instructions. Also, a data transfer from controller to processor does not require an independent legal basis. Rather, it suffices that you implement a data processor agreement that ensures the processor only acts on behalf of the controller. A template for such a processor agreement is available in the legal department. In case of a transfer from controller to controller, on the other hand, you need a legal basis for the transfer, i.e. either it is permitted by law or you have data subject consent.

Topic	Controller	Processor
Definition acc. to GDPR	According to Art. 4 No. 7 GDPR 'controller' means the natural or legal person, public authority, agency or other body which, **alone or jointly** with other, **determines the purposes and means** of the processing of personal data.	According to Art. 4 No. 8 GDPR 'processor' means a natural or legal person, public authority, agency or other body which processes personal data **on behalf of the controller**.
Legal form	The legal form (natural person, entity) of the controller is irrelevant.	The legal form (natural person, entity) of the processor is irrelevant. However, a processor would always be someone outside the organization of the controller. When we say 'organization' we mean the legal entity. I.e. any disclosure of data to another group company would also require either a controller-processor relationship or a legal basis for such data transfer.
Main differentiator	The controller determines the business 'purpose' for which ("why") the data shall be used and the 'means' in which ("how") the data are processed. You could say the controller is the 'owner' of the data. The processor, on the other hand, is bound by the instructions given by the controller and only acts 'on behalf of' the controller while processing the controller's data. I.e. the processor may not process the data for its own business purpose as this would make it (also) a controller.	
Other indicators	**The following criteria can help you to identify controllership:** ■ 'Decision-maker' as it decides on: ▪ Initial collection and why (for what purpose) personal data are collected ▪ The kind of personal data and the relevant categories of data subjects (e.g. customers, employees) ▪ To whom data may be disclosed ▪ Who shall have access to the data ▪ How long it is stored ▪ Which software/hardware is used to process the data ■ 'Owns' the data and can decide whether and how it is deleted, corrected etc. ■ 'face to the data subject': ▪ Named in the contract or consent declaration as a contractual party, named on the website by which data is collected ▪ Acts in its own name when approaching the data subject ▪ Fulfils the data subject rights (e.g. provides notice, answers access requests, is responsible for data breach notifications)	**The following criteria can help to identify a processor:** ■ 'Extended arm' of controller, mere supporting function, no decision-making power: ▪ Only obtains the data to perform processing operation for business purposes of the controller ▪ Subject to detailed instructions and guidance ▪ No decision-making power regarding the use of the personal data, in particular may not use it in its own interest/for its own business purposes ■ 'Face to the controller', as it has no business relationship with data subjects and/or when approaching the data subject only acts in the name of the controller (e.g. call center that places calls in the name of the controller.) *Please note that in this assessment the emphasis should be on who decides **on the purposes** for which data are processed. Whereas, concerning the decision on the means of processing, the service may require that the processor obtains some kind of discretion without losing the qualification as a processor (for example, a cloud processor).* **This could include decision making power on the following aspects:** ■ What IT systems, hard- or software or other methods to use ■ How data is stored ■ Details of the security measures ■ Means used to transfer the personal data to a recipient ■ The methods used to guarantee a retention schedule ■ The means used to delete the personal data

Topic	Controller	Processor
Examples	■ Employer re. data of its employees ■ Contractual party re. customer data ■ Social network providers in relation to members' data **A controller-to-controller transfer, for example would be:** ■ Lawyers, auditors, tax consultants as provision of their services requires that they have own decision-making power in performing their services; they usually have their own legal basis for such data processing ■ Headhunter who sends 'candidates' data, as the headhunter would always keep the personal data for its own business purposes A 'joint controllership' requires that the controllers jointly decide on the purposes and means of the processing. This could be the case if legal entities share the same pool of data in a central database.	■ Hosting and maintenance by IT service providers ■ Software integrations ■ Sending marketing material to the controller's customers in the controller's name ■ Managing payroll for controller's business ■ Archiving services ■ Call center, but only in case the controller gives detailed instructions and the call center has to present itself using the identity of the controller when calling the controller's customer
Borderline Cases	■ Debt collection agency: The classification depends on how detailed the instructions are (decision making power yes/no). In case the agency only sends out pre-prepared reminders, it is a processor. In case the agency is allowed to make legal decisions on its own or represents the company in front of court, it qualifies as a controller. ■ Professional services (e.g. consultancy firms, incl. auditors providing consultancy advice) can be determined as a controller in case it is only possible to provide them with very general instructions and/or services require that they decide on the 'purpose' of the data processing (e.g. because they use their own methodology for certain analytics). However, in case it is possible to provide detailed instructions e.g. on how to conduct an audit, they can qualify as a processor. ■ To sum it up: Detailed instructions are key indicators for a controller-processor relationship.	

Your Contacts

Dr. Axel Frhr. von dem Bussche, LL.M. (L.S.E.)
Tel +49 (0)40 3 68 03 347
a.bussche@taylorwessing.com

Global Leader for Data Protection
Who's Who Legal 2020

Leading individual for IT and Digitalization – Germany
Legal 500 Germany 2020

Leading individual for TMT: **Data Protection**
Chambers Europe 2020

Dr. Paul Voigt, Lic. en Derecho, CIPP/E
Tel +49 (0)30 88 56 36 408
p.voigt@taylorwessing.com

Highlighted as Lawyer of the year 2020
Data protection law, Best Lawyers in Germany, Handelsblatt

Next Generation Lawyer – Germany
Legal 500 Germany 2020

TOP Lawyer for **Data Protection Law**
WirtschaftsWoche 2019

TaylorWessing

16 jurisdictions

28 offices

300+ partners

1000+ lawyers

Austria	Vienna I Klagenfurt*
Belgium	Brussels
China	Beijing* I Hong Kong I Shanghai*
Czech Republic	Prague I Brno*
France	Paris
Germany	Berlin I Düsseldorf I Frankfurt I Hamburg I Munich
Hungary	Budapest
Netherlands	Amsterdam I Eindhoven
Poland	Warsaw
Slovakia	Bratislava
South Korea	Seoul**
Ukraine	Kyiv
UAE	Dubai
United Kingdom	Cambridge I Liverpool I London | London Tech City
USA	Silicon Valley* I New York*

* Representative offices
** Associated office