privacyofficers.at

Role model of the Austrian company and public authority data protection officers

(VO [EU] 2016/679)

Version: 2.0
Status: December 2021

Imprint: Media owner, publisher and producer: Association of Austrian company and official data protection officers - Privacyofficers.at, ZVR number 061847005, Vienna, https://www.privacyofficers.at/impressum

Foreword of the Board of Directors

Dear Reader,

The Association of Austrian Data Protection Officers - Privacyofficers.at is pleased to provide the role model of the Austrian Data Protection Officers. This version is a first further development of the original paper of 2017 and takes into account important decisions in case law as well as experiences in the practice of data protection officers since the entry into force of the GDPR. In the present version, the Austrian Data Protection Amendment Act 2018 has been taken into account accordingly.

The present work deals with the topics of the appointment of the data protection officer(s) (e.g.: "Who must/who can appoint one?", "What requirements in professional, social and other respects must a data protection officer fulfil?"), the position of the data protection officer in the exercise of his/her function, where/how the data protection officer should be positioned in the organization, delimitation of the tasks of the data protection officer to other positions in the organization, the position of the data protection officer under employment law and, of course, the tasks of the data protection officer.

Of course, data protection officers in authorities and public bodies are also taken into account.

Finally, we have attached a sample template for the appointment of a person as data protection officer.

The present work is not to be regarded as static, but as a living work which will be subject to constant revision. Nor does the present role model claim to offer a solution to all questions in connection with the data protection officer. Our aim was to address and elaborate on the most important and practically relevant points in a compact and clear form. Thus, we have revised and adapted the role model for this version 2 in 2021.

We hope that this role model will help data controllers and processors with the questions of whether and how to appoint a data protection officer, what requirements the officer must meet, what his/her tasks are, how the officer is to be or can be integrated into the organization, etc.

We are happy to receive suggestions and constructive criticism at office@privacyofficers.at. You can find the latest data protection news on our homepage: https://www.privacyofficers.at/.

The development of the first version of the role model would not have been possible without the commitment of our working group. We would therefore like to express our special thanks to the members of the working group "Role Model for Data Protection Officers Austria", headed by Dr. Natalie Ségur-Carbanac, for their active cooperation and preparation of this role model.

The board of the association

and the authors exclude all liability, whether in contract, tort (including negligence) and/or any other legal theory, for any loss or damage, including loss of profit or any other direct or indirect consequential loss, arising out of or in connection with the use of or reliance on the information provided in this document, or any failure to act on any information contained herein.

Table of Contents

Role model of the Austrian company and public authority data protection officers

Introduction

With the General Data Protection Regulation (EU 2016/679) coming into force on 25 May 2018, there have been many new challenges for anyone processing personal data. One of the key figures for a successful enforcement of data protection law is the data protection officer. Since then, the function of the data protection officer(s) has also existed in Austria, and some companies have had to and must appoint them on a mandatory basis. The Privacyofficers.at association sees itself as an association of Austrian company and official data protection officers with the aim of offering this new professional group appropriate support in establishing and carrying out their tasks and functions.
In this role model, we want to describe the provisions of the GDPR on the function of the data protection officer for Austria and thus contribute to a uniform establishment of the data protection officer in Austria. The legal views formulated in this document are without prejudice to future decisions of the highest courts; rather, they are intended to help consolidate the job description of the data protection officer both in practice and in the relevant legal bases. The role model is intended to be a living document that will be modified/adapted by the authors as needed.

1 Appointment of the data protection officer(s)

Article 37 of the GDPR provides for the mandatory appointment of a data protection officer in three cases. Both controllers and processors must appoint a data protection officer if

a) the processing is carried out by a public authority or body, with the exception of courts acting in the exercise of their judicial functions,
b) the core activity of the controller or processor consists in carrying out processing operations which, by virtue of their nature, their scope and/or their purposes, require extensive regular and systematic monitoring of data subjects, or
c) the core activity of the controller or processor consists in the extensive processing of special categories of data pursuant to Article 9 GDPR or of personal data relating to criminal convictions and offences pursuant to Art 10 GDPR.

1.1 Processing by a public authority or body

Art 37(1)(a) of the GDPR provides that "public authorities and public bodies" (with the exception of the courts in the case of judicial activities) must appoint data protection officers.
The understanding of what is meant by "public authorities and public bodies" depends on national law:
In Austria, "public authorities" are legally regulated institutions that are called upon to carry out certain public tasks, regardless of their legal form. In this respect, this term largely corresponds to the already existing term of the "contracting authority in the public sector" according to Section 5 (2) DPA 2000, which does not distinguish whether the contracting authority is established in the form of public or private law, as long as the data use takes place "in execution of the law".

Public bodies" are all bodies according to Section 4 of the IWG. The term "public sector body" thus corresponds to the term "public sector body" in Art 2 of the PSI Directive 2003/98/EC, [1]which was transposed into national law by the IWG. In terms of content, this term, without explicitly referring to it, is equivalent to the term "public contracting authority" according to Section 3 (1) BVergG 2006. In summary, it can be said that in addition to public authorities and entrusted companies, companies that are subject to public procurement law are also obliged to appoint a data protection officer.
In addition to this obligation, the Article 29 Working Party recommends [2]that companies performing "public tasks", i.e. providing daily services to the public, such as water or energy supply, road infrastructure, etc., should also appoint a data protection officer. This is because the data subject will be in a comparable situation vis-à-vis these companies as vis-à-vis a "public authority or body". It should also be noted that in its guidance on the GDPR, the DPA refers, [3]inter alia, to the definition of public sector controller in Section 26(1) of the GDPR.

1.1. Core activity

For the obligation to appoint a data protection officer - apart from authorities and public bodies - Article 37 (1) (b) and (c) GDPR refers to the term "core activity". However, there is no definition in the GDPR of this essential criterion. Since the term is only used outside the GDPR in Directive 2013/36/EU[4] and the associated Regulation 1151/2014[5] - and is not defined there either - as well as any case law on autonomous interpretation by the ECJ is missing to date, corresponding guidelines and interpretation aids are of great importance, especially in this area.

Only recital 97, which can be used for interpretation, defines the core activity as the main activity of the person responsible in the private sector. This excludes mere ancillary activities. Accompanying - albeit necessary - administrative control or other maintenance measures are therefore not to be considered as core activities (e.g. accompanying video surveillance in the warehouse of a production facility). This probably applies in general to the area of own employee data management, provided that the person responsible is not a recruitment agency. However, it remains unclear which activity focus or which parameters (e.g. turnover, size of the department, investments, etc.) are to be taken into account if a controller is primarily active in several economic sectors.

In its Working Paper 243, the Art 29 Data Protection Working Party also offers further delimitation criteria, which, however, lead to a broad interpretation of applicability: Core activities are supposed to be all those activities of a controller that constitute "an inseparable part" of the main activity of the company in pursuit of the company's objectives. Again as a negative delimitation, the Art 29 Working Party also follows the view that processing of employee data - which is bound to be extensive and regular in any larger company - is merely a subsidiary ancillary activity. With regard to the requirement of monitoring individuals, however, it also points out that, in addition to classic video surveillance, this is in particular online tracking and profiling for target group-oriented advertising and e-mail retargeting.

---

[1] This is also pointed out by the Art 29 Working Party in WP 243 rev.01, 6 (FN 11).
[2] http://ec.europa.eu/newsroom/document.cfm?doc_id=43823 in point 2 of the Annex to WP 243
3 (as of July 2017) 31 f.
4 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:176:0338:0436:DE:PDF
5 http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R1151&from=DE

In summary, the core activity can be defined as the key activity for achieving the company priorities or objectives set by the controller. In this context, the data processing itself does not have to constitute the core activity. Ultimately, it boils down to a demarcation between a merely incidental processing and one that represents an inseparable part of achieving the objective.

1.2 Who may be appointed as data protection officer(s)

Pursuant to Art 38(5) GDPR, the Data Protection Officer shall be appointed on the basis of his/her professional qualifications and, in particular, the expertise he/she possesses in the field of data protection law and practice, as well as on the basis of his/her ability to perform the tasks referred to in Art 39 GDPR.

The data protection officer must have sufficient expertise and professional qualifications in data protection law and practice. These requirements can only be met by persons who have knowledge in the areas of law, organisation and technology. In addition, social skills are an essential factor for holding the position of data protection officer(s). The data protection officer should also have professional experience in one of the above-mentioned areas (legal, organizational, technical). The level of expertise required should depend in particular on the data processing operations carried out and the protection required for the personal data processed by the controller or processor.

In the area of law, a data protection officer should at least be able to cover the following legal matters with confidence:

- Fundamental rights, in particular Art 8 ECHR and Art 7 and 8 CFR
- EU General Data Protection Regulation
- Data Protection Act 2018
- Planned e-privacy regulation
- Telecommunications Act 2003, in particular Articles 92 to 107 TKG 2003
- Legal basis for data processing, retention and deletion periods
- Special legal provisions regarding data protection (e.g. Health Telematics Act, Health Telematics Ordinance)
- Labour constitution law, in particular §§ 91, 96, 96a and 97 ArbVG
- Contract law

In the area of technology, the data protection officer should have at least basic knowledge in the following subject areas:

- Functioning of modern information and communication technologies (Internet, e-mail, over-the-top communication services, cloud services)
- Security risks, especially social engineering (e.g. phishing) and malware (e.g. viruses, Trojans, spyware, ransomware)
- Information security management systems (e.g. ISO/IEC 27001:2013) and information security measures

In the area of organization, the Supervisor should be familiar with the following disciplines of management theory:

- Audit Technology
- Continuing education and awareness raising
- Project and process management

The DPO should also have a good overview of his/her organisation and have extensive knowledge of the core business and processes. This will make it much easier for the DPO to have access to the relevant data processing operations in his/her organisation and to advise on issues at an early stage.

The requirements for future data protection officers are very high. The data protection officer must have extensive knowledge in complex areas. For almost every data protection officer, regular attendance of further training will be indispensable in the coming years. Lawyers will need to catch up in the areas of technology and organization. Data protection officers with a different educational background will have to expand their (data protection) legal knowledge. The organizations must make the necessary resources available to the data protection officer.

The data protection officer must perform important "translation work". He/she will be confronted with technical, legal and organizational problems. For this reason, the clear recommendation is made at this point that companies also provide the data protection officer with further training in the area of social skills (communication and conflict resolution skills as well as moderation and mediation techniques).
More generally, in our view, such training courses financed or facilitated by the company should not - as is common practice - be made subject to commitment or repayment obligations on the part of the data protection officer. This contradicts the independence and freedom of instruction to be guaranteed, since a data protection officer may be restricted in his/her freedom of movement with the prospect of having to repay a training course. This applies at least to those training courses which the controller must finance on the basis of Art 38 GDPR. It would be absurd to ultimately make the data protection officer pay for this.

1.3 Constellation of controller/processor and enterprise groups:

If data processing is carried out in a contract processing relationship, the controller and processor must consider on the basis of the specified criteria whether the appointment of a data protection officer is necessary or whether only one of the two parties is obliged to do so. It is advisable to clarify this contractually. Particular attention will have to be paid to where and how the data is actually processed, as well as who bears the actual risk of data processing.

Pursuant to Art 37(2) GDPR, a group of undertakings may appoint a joint data protection officer, provided that this officer can be easily reached by each establishment. A group of undertakings consists of a controlling undertaking and undertakings that are independent of it, with the controlling undertaking having the power to have data protection rules implemented (cf. Art 4(19) GDPR, recital 37). In which cases a dominant position of a company exists is a question of company law and thus left to the respective national legal system, whereby the relevant company law provisions including case law, in particular Section 244 UGB and Section 15 AktG, are relevant for Austria.

The aim of joint data protection officers is also the easy possibility to contact them and to make use of their advice. Criteria for the accessibility mentioned are therefore physical and media accessibility as well as the absence of language barriers. In international groups of companies, this last characteristic will make it difficult to centralize tasks completely, in particular because it will not be possible to contact customers in all the languages of the countries in which the group of companies is located, and it will hardly be possible for the data protection officer to communicate with the authority in the official language of the respective country.

Authorities and public bodies may also appoint a joint data protection officer. The criterion here is that the size and organisational structure of these authorities or public bodies should be taken into account. This indicates that in particular an equal portfolio of legally assigned tasks should promote this joint appointment, as is the case for example with municipalities, district authorities or smaller district courts.

The wording of Art 37 (2) GDPR indicates that the required appointment of the data protection officer(s) vis-à-vis the supervisory authority by the controlling company of the group of companies is sufficient.

The data protection officer can either be appointed internally from among the company's own employees (internal data protection officer) or an external person or company can be entrusted with this role (external data protection officer). All persons of this external company entrusted with DPO tasks must comply with all requirements of the GDPR (e.g. none of these persons may have a conflict of interest with other tasks). Conversely, all these persons must be protected to the same extent by the GDPR (e.g. no termination of the contract of employment because of the activity as DPO). With regard to legal certainty and good organisation, it is recommended that in such teams of data protection officers, which can work together more efficiently due to different skills and strengths, the tasks in the team are clearly allocated (e.g. contractually or by guidelines) and one person is defined as the main contact or responsible for each request (Guidelines on Data Protection Officers, p 12). The external data protection officer will have access to personal data of the respective client within the scope of his/her activities (cf. Art. 38 (2) GDPR). It remains to be seen whether this will additionally establish a separate order processing relationship - with all the consequences (conclusion of an order processing contract, etc.). This would probably not be compatible with the freedom of instruction and independence of the (external) data protection officer(s).

A joint data protection officer of controllers and processors is also conceivable, but will find its limits in conflicts of interest where the advisory and supervisory activities are made difficult or impossible by different interests (e.g. in the risk assessment of a project). Such constellations must therefore be decided on a case-by-case basis, taking potential conflicts of interest into account.

1.4 How to appoint the data protection officer(s)

In any case, it is recommended to make a written appointment. A template for the appointment of a data protection officer can be found in Appendix 1 of this document.

The contact details of the data protection officer(s) must be published and communicated to the supervisory authority. The best way to publish contact details is to include them on the company's website or, for employees, on the intranet site. It is not absolutely necessary to provide personal telephone numbers or e-mail addresses of the data protection officer(s). It must be ensured that data subjects can simply contact the data protection officer(s) via the contact data provided (general telephone number, general e-mail address of the data protection officer(s), such as datenschutzbeauftragte/r@.... at) can easily reach the data protection officer and also enter into dialogue.
The person of the data protection officer(s) must be named to the data protection authority. Here, the Austrian data protection authority requires brief information about the name of the company and the name of the appointed person after consultation, whereby an informal notification by e-mail to the data protection authority (dsb@dsb.gv.at) is sufficient.

1.5 Integration of the data protection officer(s) into the company organisation

The GDPR allows for the appointment of both an internal employee and an external service provider (Art. 37 (6) GDPR). In practice, it should be ensured that the data protection officer can perform his/her duties as effectively as possible. It may well make sense to divide the tasks of the data protection officer among more than one person. One possible solution would be to appoint an external data protection officer and at the same time nominate an internal contact person, who would then jointly address and take care of the topic of data protection in the company. The combination of internal and external experts can also have positive side effects, for example through the combination of deeper knowledge of the organization from the inside with objective insight from the outside. In turn, external service providers who serve multiple data controllers and/or processors can bring their experience with different industries and companies to the work with the individual controller. Even without the involvement of external consultants, a division of tasks can be sensibly set up, e.g. by forming a committee of experts from different areas of the company but also with different tasks within the company (compliance, information security, human resources management, works council, etc.) to support the data protection officer(s).

2 Position of the Data Protection Officer(s)

The data protection officer is a key figure for the successful implementation of the requirements of the GDPR in Europe. In this respect, the GDPR grants the data protection officer corresponding special features when it comes to the position in the organisational structure and in the integration in the corporate decision-making processes that are in any way related to the protection of personal data. The data protection officer must be involved at an early stage and the organisation must ensure his/her independence and freedom from instructions (see Art. 39 GDPR).

2.1 Independence and freedom from instructions

According to Art. 38 No. 3 GDPR, the data protection officer is free from instructions with regard to the performance of his/her tasks and may not be dismissed or disadvantaged for reasons related to the performance of his/her tasks. These privileges are intended to ensure that the data protection officer can carry out his/her duties without interference. It is irrelevant whether the appointment of the data protection officer is voluntary or mandatory. For companies, this results in the need to

carefully examine a possible external or internal data protection officer before entrusting him or her with the task. In order for a company to be able to react to changes in the company environment despite being bound to a data protection officer, it is recommended that the appointment of the data protection officer be limited in time. However, existing case law in countries where there are already mandatory data protection officers, in particular Germany, requires a minimum period of time for this, which enables the data protection officer to perform his/her duties in a meaningful way. For internal data protection officers, a period of two to five years is considered sufficient. For external data protection officers, an initial contract with a term of one to two years is recommended, followed by contracts with a term of four years. A shorter term in the sense of a probationary period was not recognized. Thus, the examination of the suitability must already be carried out thoroughly before the appointment.

2.2 Freedom from instructions

Labor law implications

In principle, the employer has the right to issue instructions to employees. This is a core element of employment relationships and the last level in the tiered structure of labour law.

It serves, among other things, to specify employment relationships such as working hours, place of work and the content of the activities to be performed. Furthermore, it includes regulations on overtime, division of working time, break regulations, holidays, company holidays, quality of work, orderly conduct (e.g. smoking ban or type of clothing), etc.

Employees can refuse to follow instructions if they violate the law or if they are harassed in any other way. So far, safety representatives, works council, board of directors and management have been exempt from instructions under Austrian labour law.

The right to issue instructions in the judiciary, on the other hand, is precisely regulated by law; instructions from the Chief Public Prosecutor's Office and the Federal Minister of Justice may only be issued in writing and with reasons.

Implications for data protection law

Article 38 (3) of the GDPR regulates the right to issue instructions to a data protection officer. The controller must ensure that the data protection officer remains free from instructions in the performance of his/her duties. The internal data protection officer is thus only exempt from the employer's right to issue instructions in the data protection area. All other instructions that are not related to this (working time and place, vacation, etc.) are not covered by this.

The Art 29 Data Protection Working Party does not give a general recommendation on how the freedom of the data protection officer(s) to issue instructions should be handled in principle, but it does give some concrete indications.

Art 38 GDPR together with Recital 97 stipulates that this freedom to issue instructions deliberately exists only for the area of the data protection officer(s).

This means that no instructions may be given only where the performance of the tasks as a data protection officer is concerned. In particular, page 15 of the Guidelines on Data Protection Officers of

the Art 29 Data Protection Working Party indicates that the DPO cannot be told how to conduct an investigation in a complaint procedure or how and when to contact the supervisory authority. This is therefore solely within the discretion of the DPO. Furthermore, a data protection officer may not be instructed on how to interpret data protection rules or what assessment to make.

The controller thus always remains responsible for compliance with data protection laws and regulations. If decisions of the controller are contrary to data protection law, the data protection officer must have access to the highest management level to explain his/her opinion and assessment.

.

3 Organisational positioning of the data protection officer(s) and potential conflicts of interest

The data protection officer may also take on other tasks in addition to his/her own activities. Care must be taken to ensure that these tasks do not lead to a conflict of interest. [6]The data protection officer shall be independent and not subject to directives. He/she monitors compliance with the data protection regulations in the company or the authority. If assigned tasks are in conflict of interest with the activity as data protection officer, this contradicts his/her independent position. The data protection officer must not be required to monitor him/herself.
When other tasks are delegated, care must also be taken to ensure that the DPO has enough time to carry out his/her duties and thus has sufficient resources to carry out his/her tasks in a meaningful way.

- Conflicts of interest may[7] exist in particular in the following cases:
  - Management of authorities and companies
  - Head of IT
  - Head of personnel
  - Head of Legal Affairs
  - Head of Marketing
  - Investigative bodies such as compliance officers or internal auditors: If they are tasked with carrying out specific control measures, this can lead to conflicts of interest. In order to perform their auditing duties, investigative bodies have an interest in having the most unrestricted access possible to data and data processing. This is the case, for example, if the internal audit department requires extensive evaluations of personal data or log data in the course of its activities. When considering whether a conflict of interest exists in the case of investigative bodies, it must also be taken into account whether or not they are free from instructions in their activities.
  - Employees, if they can determine or significantly influence data processing processes (e.g. in IT or human resources)

[6] Art 38 Abs 6 DSGVO
[7] We point out potential conflicts of interest, which have to be examined and weighed up in each individual case and then, depending on the result, may or may not exist.

- Organisational units with particularly extensive processing of personal data or processing of special categories of personal data pursuant to Art. 9 GDPR (e.g. responsibility for Big Data applications)
- Works council: In the case of the works council, it is debatable whether there is a conflict of interest. This must be carefully weighed up. There is a risk that decisions are made in accordance with employment law requirements and that this leads to a conflict of interest with data protection. According to the GDPR, the data protection officer must be involved by the controller or processor as early as possible. In the case of the works council, there is no guarantee that it will receive all information on the topic of employee data processing at an early stage. In addition, the role of a works council is to represent all employees; the data protection officer must also safeguard the interests of the company and other data subjects.

In principle, it is useful to document where conflicts of interest exist. It should also be recorded how much time the activity as data protection officer takes up. These parameters should be taken into account accordingly when filling the position.

3.1 Necessary resources of the data protection officer(s)

Controllers and processors are obliged to assist the DPO in fulfilling the obligations listed in Art 39 GDPR by providing him/her with the resources and access to all relevant information necessary for the performance of these tasks. It is therefore inadmissible in any case, in order to prevent unpleasant recommendations, not to inform the DPO or to inform him/her only selectively about planned data uses. At the same time, this is also impracticable and would, to a certain extent, reduce the position of the data protection officer to absurdity.

Resources that have to be made available also include staff, budget, premises. Neither for the number of employees nor for the budget size are there general rules - it depends here on the individual case of the company's activity and the number and complexity of the issues in practice.

However, the following point of reference can be used for large companies: The German Federal Commissioner for Data Protection and Freedom of Information recommends the full exemption of one person for public bodies with 1,000 or more employees. For small and medium-sized enterprises, sole proprietors or start-ups for information society services, this number does not represent a measure. Conversely, consideration should be given here to providing the designated data protection officer, who is not working to full capacity, with other tasks that are not incompatible.

In addition to human resources, the Art 29 Data Protection Working Party sees the following issues in focus in the Guidelines on Data Protection Officers, p 13f:

- Active support of the data protection officer(s) by the executives of the organisation (e.g. the board of directors)
- Support in the form of a budget and infrastructure (office space or equipment)
- Communicate the appointment and contact details of the Data Protection Officer(s) to all employees to make their existence and role known.

- Access to other areas of the company such as human resources, legal, IT, information security, etc. to provide the data protection officer with the necessary support and information.
- Continuous training, in particular as regards developments in the field of data protection (e.g. via seminars, interest groups, workshops, etc.).

The more complex or sensitive the data processing of an organisation is, the more resources must be made available to the data protection officer. The data protection function must be efficient and adequately resourced in relation to the data processing and the associated risk to data subjects.

With regard to the resources for maintaining the expertise, there are also no detailed specifications - here, too, much ultimately depends on company practice. This will probably only apply to internal data protection officers, i.e. those appointed from within the company or group of companies, and not to external service providers. In the (not adopted) draft amendment to the Austrian Data Protection Act 2000 from 2012 (Section 17a (8) of the draft amendment to the Data Protection Act 2012), the data protection officer was to be provided with 40 hours of training, and in each subsequent year with 20 hours of training. These ideas can, of course, also serve as - non-binding - support for the practical design after the GDPR.

3.2 Responsibility of the Data Protection Officer(s)

The role of data protection officers is designed as an advisory body on all data protection issues. In addition to the tasks listed in Art 39 GDPR, the data protection officer may also take on other tasks as long as this does not lead to incompatibilities.
If these 'other tasks' were management tasks related to the use of personal data, the DPO would thus be in the situation of having to advise himself/herself, which would be in conflict with the concept of an independent DPO with institutional safeguards.

This means that the data protection officer can therefore never make ultimately responsible decisions on how personal data are used (including the internal group guidelines on this) and that a corresponding decision-making power must automatically lead to a conflict of interest between the "advisor" and the "decision-maker".

This further means that the data protection officer can never be appointed as the "responsible officer" pursuant to Section 9 VStG as far as violations of data protection law are concerned, because the legal prerequisite for this is the "corresponding authority to issue orders", which would have enabled the appointed officer to avert the violation of administrative criminal law (in this case data protection law).[8] However, this is in stark contrast to the role of the data protection officer(s).

[8] See also the Guide to the GDPR of the Austrian Data Protection Authority (p. 32 f) at https://www.dsb.gv.at/documents/22758/116802/DSGVO-2016-Leitfaden.pdf/93d6cb80-8d8e-433d-a492-a827e3ed81a2.

The controller or processor is responsible for compliance with the GDPR. Only the latter can be the addressee of the penalties/fines pursuant to 83ff GDPR. [9]

The Data Protection Officer shall therefore only be responsible for the tasks referred to in point 6above.

4 Delimitation of the tasks of the data protection officer to other positions in the organisation

We recommend a clear description of the tasks of the data protection officer. The tasks that a data protection officer has to perform in the context of a data protection organisation overlap per se with already known roles in an organisation, such as compliance and information security. The Art 29 Working Party[10] even requires basic knowledge of the data protection officer in these areas. In order to avoid both negative and positive conflicts of competence, the tasks of these functions should be described very precisely and assigned to the respective responsible persons in an organization. In any case, cooperation between these persons is recommended in practice.

5 Employment status of the data protection officer(s)

In the Data Protection Amendment Act 2018[11], the legislator did not provide for a special position of the data protection officer under employment law. However, based on the provisions of Article 38 (3) of the GDPR, it can be assumed that the data protection officer is entitled to a so-called protection against dismissal on grounds of motive, as is the case under Austrian law in other cases: Here, there are persons with special protection against dismissal enshrined in law[12]. In the case of these employees, dismissal is only permitted with the approval of the court/Federal Social Office. There is no such provision for data protection officers. In order to grant data protection officers the same legal status with regard to protection against dismissal and dismissal, an explicit legal regulation would be required. This is lacking. The position of the data protection officer can best be compared to that of the safety representative[13]. This person is also exempt from instructions by law. If a safety representative is dismissed or made redundant, he or she can challenge the dismissal or redundancy in court if it was because of his or her work on the safety and health of workers. It is questionable whether a DPO without a statutory basis will also be able to rely on this legal protection. We assume that Art 38(3) GDPR can only have full direct effect if the DPO is actually granted this position in the context of termination and dismissal scenarios. Thus, the dismissed/dismissed data protection officer would have to be allowed to challenge an unlawful termination/dismissal in court.

[9] See Art 5(2) GDPR: "The controller is responsible for compliance with paragraph 1 and must be able to demonstrate compliance ("accountability")." As well as Art 24 in conjunction with EC 74 GDPR.
[10] http://ec.europa.eu/newsroom/document.cfm?doc_id=43823
[11] BGBl I 2017/120.
[12] Expectant mothers as well as mothers and fathers who take maternity leave or part-time employment on the occasion of the birth (part-time parental leave), works councils or equivalent persons, persons on compulsory military or civilian service as well as women in training, beneficiaries of disability and victim welfare services as well as caretakers are entitled to special protection against dismissal.
[13] Ordinance of the Federal Minister of Labour and Social Affairs on safety officers (SVP-VO)
StF: Federal Law Gazette No. 172/1996, amended by Federal Law Gazette II No. 324/2014

External data protection officers

The view of the Art 29 Data Protection Working Party, which extends the special protection against dismissal to the relationship between the client and the external data protection officer on the basis of a service contract, should not be disregarded. Even if it is questionable whether this will actually be confirmed in practice by the competent courts, it is legally stringent that the GDPR itself does not make any distinction in the regulation of Art 38 (3) GDPR. In order to generate unnecessary contractual conflicts, it is advisable, especially in the case of external data protection officers, to appoint them for a limited period of time (see also item 2.1).

6 Tasks of the data protection officer(s)

6.1 Contact tasks

The data protection officer is the central contact person for the data protection or supervisory authority. In this context, special attention will have to be paid to how the data protection officer presents him/herself to the data protection authority, whereby he/she must ensure that he/she actually only performs a coordinating and hub role and does not also act as a "representative" of the controller's organisation. The latter would conflict with the position of the DPO as an independent and noninstructive advisory body. The data protection officer should therefore avoid clearly communicating personal legal views or perceptions of facts as such and not give the impression that he or she is expressing or representing the opinions of the company. At the same time, however, he/she should also regularly coordinate internally so as not to torpedo strategic considerations.

6.2 Advisory, monitoring and training functions

The data protection officer also has an advisory, supervisory and training function within the company:

Consulting

The Data Protection Officer shall thus inform and advise on

- the management,
- the staff involved in the processing of personal data
- all employees as affected persons
- the works council (if any), e.g. in the case of corresponding works agreements
- upon request, the responsible persons in carrying out the data protection impact assessment.

Monitoring

The data protection officer shall monitor compliance with all provisions of data protection law, such as

- GDPR
- Other EU data protection legislation (e.g. ePrivacy Directive)
- National laws (e.g. Data Protection Act, Telecommunications Act, Labour Relations Act, E-Commerce Act, Health Telematics Act, etc.).)

This monitoring obligation concerns the audit of the relevant processes and procedures to meet the requirements of the GDPR, such as

- Processes for the exercise of data subjects' rights
- Process for informing the public and the persons concerned
- Development processes (data protection by design)
- Checking the permissibility of processing in the case of new software to be implemented

However, this monitoring obligation also concerns the examination of the required documents and contracts, such as

- Procedure directory
- Order processing contracts
- EU standard contractual clauses for data transfer to third countries
- Data protection declarations and legally effective declarations of consent
- Obligation of employees to comply with data protection
- Internal guidelines for handling IT assets

Special aspects of monitoring are the examination of technical measures[14].

Regardless of the size of the company, the monitoring activity is best performed by means of a data protection audit to be carried out at least once a year by the data protection officer or by a data protection audit commissioned by him/her. The result of the audit is sent as a report to the management and also contains the proposed measures to be implemented on the basis of the deviations found.

Active activity

The DPO should actively participate in the preparation and possibly also in the delivery of the Awarenes training. [15]

Cooperation with the supervisory authority; point of contact for the supervisory authority.

7 Data protection officers in authorities and public bodies

The explanations in this document essentially also apply to the appointment, position and tasks of data protection officers in public bodies. The Data Protection Act 2018 provides for a few special features for "public" data protection officers: For example, they are also expressly exempt from instructions and should be able to perform their duties independently (Section 5(2) DSG). In the sphere of action of ministries and these downstream bodies, data protection officers must come directly from these institutions; the appointment of other data protection officers, including external

[14] See the Privacyofficers.at checklist at https://www.privacyofficers.at/privacyofficers-at-veroeffentlicht-checkliste-zur-umsetzung-der-dsgvo/.

[15] Note: In medium-sized and smaller companies, these procedures and documents are rarely in place. Here, the data protection officer will probably be more sensibly involved in the creation of the documents.

ones, is inadmissible here in any case. [16]Finally, data protection officers in the public sector are legally required by Section 5(3) of the Data Protection Act to maintain a regular exchange of experience with a view to ensuring a uniform standard of data protection. [17]

Data protection officers in the public sector have a seat on the Data Protection Council (Section 21(6) of the FADP).

Data protection officers must report to the highest management. In the public sector, it is to be assumed that this is the minister himself/herself or the comparable top executive function in an administrative organisation (federal government, Länder, municipalities).

---

[16] Even if this is in line with the view of the Art 29 Working Party in its guideline on data protection officers, according to which a data protection officer of public authorities and bodies should also know and be able to have the relevant knowledge of administrative procedures and processes within the administration, we see no reason to exclude external data protection officers here by law. The latter could also bring such knowledge and experience.

[17] Here we refer to the regular network meetings and internal association seminars of Privacyofficers.at.

Sample template for the appointment of a person as data protection officer pursuant to Article 37 of the GDPR in conjunction with Section 5 of the GDPR

Appointment as Data Protection Officer pursuant to Article 37 (1) of the Data Protection Regulation in conjunction with Section 5 of the General Data Protection Regulation (EU 2016/679).

Mr/Mrs [*insert name*]_____ is appointed as data protection officer within the meaning of Article 37 et seq DSGVO with effect from [*date*].

The order relates to the company/organisation/authority [*insert name*].

The appointment is made for an indefinite period / limited until [*insert date*].

The appointment as data protection officer may be revoked at any time for good cause or at the request of the supervisory authority. In any case, the appointment shall end at the latest upon termination of the (service) contract existing between Mr/Mrs [*insert name*] and [*insert name of employer*].
Reference may be made to the duty of secrecy (without prejudice to other duties of confidentiality) and the right to refuse to give evidence in the performance of your duties pursuant to Section 5 of the Data Protection Act.

[Signature of management]

I hereby accept my appointment as Data Protection Officer in accordance with the above content.
I hereby take note that according to Art 37 (7) DSGVO, the contact details of the data protection officer (e-mail address, telephone number and address) must be published by the employer and these must also be communicated to the data protection authority.

Place, date
[Signature of Data Protection Officer]