Role model of the Austrian operational and governmental data protection officers

(VO [EU] 2016/679)

Version: 1.0
Status: October 2017

Legal notice: Media owner, editor and producer: Austrian Association of operational and governmental data protection officers - Privacyoffiicers.at, ZVR-number (Central Associations Register) 061847005, Vienna, https://www.privacyofficers.at/Legal notice

Preface of the Executive Board of the Association

Dear reader,

The Austrian Association of operational and governmental data protection officers Privacyofficers.at is pleased to be able to provide this role model of the Austrian operational and governmental data protection officers. In the present version the Austrian Data Protection Amendment Act 2018 has been incorporated accordingly.

The present work deals with the issues of appointing the data protection officer/s (e.g. "Who needs to/can appoint one?", "Which requirements does a data protection officer need to meet in terms of professional, social and other skills?"), the position of the data protection officer/s in the execution of his/her duties, where/how the data protection officer should be positioned organizationally, differentiation of the duties of the data protection officer from other positions within the organisation, the employment-related position of the data protection officer and of course the tasks of the data protection officer.

As a matter of fact, data protection officers with authorities and official bodies are equally considered.

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

The present work shall not be considered static, but as a living work which will be revised consistently. The present role model does not claim to offer a solution to all questions connected with the data protection officer. It was our goal to treat in a compact and clear form the most important and practice-relevant items and to elaborate these.

We hope that the present role model will support the responsible persons and data processing companies with the questions whether and how a data protection officer should be appointed, which requirements he/she has to meet, which are his/her tasks, how he/she has to be integrated into the organization, resp. how he/she may be integrated etc..

We are happy to receive suggestions and positive critical comments under office@privacyofficers.at, current data protection news can be viewed on our website: https://www.privacyofficers.at/.

The elaboration of the role model would not have been possible without the efforts of our study group. We therefore explicitly express our thanks to the members of the study group "Role model Data Protection Officers Austria" under the direction of Dr. Natalie Ségur-Cabanac for their active cooperation and drawing up of this role model.

Executive Board of the Association

or other direct or indirect secondary damages which derive from the use of or the reliance on the information provided in the present document or from a possible non-consideration of certain information.

Table of contents

Role model of the Austrian operational and governmental data protection officers

Introduction

With the General Data Protection Regulation (EU 2016/679) coming into force on May 25, 2018, new challenges will arise for anybody/any entity processing personal data. One of the key figures for a successful execution of the data protection law is the data protection officer. In Austria the new position of the data protection officer will come into existence which some enterprises will be obligated to appoint. The Association Privacyofficers.at understands itself as interest association of the Austrian operational and governmental data protection officers having the goal to offer appropriate support to this new professional group with the establishment and performance of their new tasks and functions.

In the present role model we want to describe the stipulations of the DSGVO (General Data Protection Regulation) regarding the role of the data protection officer for Austria and by such contribute to a uniform establishment of the data protection officer in Austria. The legal opinions expressed in the present document are without prejudice on future Supreme Court decisions, they shall rather help consolidate the occupational profile of the data protection officer in practice as well as in the respective legal bases. The role model shall be perceived as a living document which will be modified/amended by the authors as needed.

1 Appointment of the data protection officer

In its Art. 37 the DSGVO basically provides the mandatory appointment of a data protection officer in three cases. The person in charge as well as the data processing company shall appoint a data protection officer, if

a) the processing is being performed by an authority or an official body, with the exception of courts acting within the scope of their judicial activity,
b) the core activity of the person in charge or the data processing company consists in the performance of processing acts which, due to their type, their extent and/or their purposes require an extensive, regular and systematic monitoring of persons concerned, or
c) the core activity of the person in charge or of the data processing company consists in the extensive processing of specific categories of data according to article 9 DSGVO or of personal data on criminal convictions and offences according to Art 10 DSGVO.

1.1 Processing by an authority or an official body

Art 37 para 1 sub-para a DSGVO provides that "authorities and official bodies" (with the exception of courts when executing judicial activities) shall appoint data protection officers.

The understanding of what shall be qualified as "authorities and official bodies" is subject to national law:

"Authorities" in Austria are legally regulated institutions summoned for the execution of certain public tasks, independent from their legal form. In this respect the term to a large extent corresponds to the already existing term of the "Principal of the Public Sector" according to § 5 para

2 DSG 2000, which does not distinguish between the principal instituted according to public or private law, as long as the data use happens "in execution of the laws".
As "official bodies" shall be deemed all bodies according to § 4 IWG (Federal Act on the re-use of public sector information). The term „official body" corresponds to the term "official body" in Art 2 of the PSI-directive 2003/98/EG,[1] which has been implemented into national law with the IWG (Federal Act on the re-use of public sector information). With regards to content this term shall, without referring to it explicitly, be equated with the term of "official principal" according to § 3 para 1 BVergG 2006 (Federal Procurement Law). Summing up it may be stated that beside authorities and attributed enterprises also enterprises subject to public procurement law, shall be obligated to appoint a data protection officer.
Beyond this obligation the Art-29-Data Protection Group recommends[2] that enterprises performing "public tasks", i.e. providing services of daily needs for the public, such as for example water- and energy supply, street infrastructure etc. shall equally appoint a data protection officer. This because the person concerned will be in a situation vis-à-vis these enterprises which is comparable to the situation vis-à-vis an "authority or an official body". It also shall be stated that the data protection authority in its code of practice to the DSGVO[3] amongst others refers to the definition of the responsible of the public sector in § 26 para 1 DSG.

1.1. Core activity

Regarding the appointment of a data protection officer - aside of authorities and official bodies - Art 37 para 1 sub-para b and c DSGVO refers to the term of "core activity". There is however no definition of this material differentiation criterion in the DSGVO. Due to the fact that outside the DSGVO the term is only used in the directive 2013/36/EU[4] and the associated regulation 1151/2014[5] - and is neither defined there, and also that to date any jurisprudence by the EUGH (European Court of Justice) to the autonomous interpretation is missing, respective guidelines and interpretation support are of great importance in this area.

Solely in ErwGr 97 (consideration reason), which might be consulted for interpretation, the core activity is described as the main activity of the person in charge for the private sector. Mere additional businesses are excluded thereby. Accompanying - although necessary - administrative controlling and other maintenance measures are therefore not to be qualified as core activities (e.g. accompanying video monitoring in the warehouse of a production site). This will generally apply for the scope of proper employees in data administration, if the person in charge is not a recruiter. It however remains unsolved which activity key aspect, resp. which parameters shall be focused on (e.g. turnover, size of the department, investments etc.), if a responsible person is active in several business areas.

The Art-29-Data Protection Group offers further differentiation criteria in its Working Paper 243, which however in total lead to a broad interpretation of applicability: As core activity shall be qualified all those activities of a person in charge, which constitute an "inseparable part" of the main

[1] Art-29-Data Protection Group in the WP 243 rev.01, 6 (FN 11) also points that out.
[2] http://ec.europa.eu/newsroom/document.cfm?doc_id=43823 in item 2 of the enclosure to WP 243
3 (Status 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

activity of the enterprise for the pursuance of enterprise goals. As a negative differentiation on the other hand the Art-29-Data Protection Group supports the opinion that a processing of employees' data - which with regard to a bigger enterprise is by necessity done in an extensive way and on a regular basis - only constitutes a subordinated auxiliary activity. Regarding the requirement of monitoring of people, it however equally shows that besides classic video monitoring this is in particular online tracking and profiling for target-group-oriented advertising and E-Mail retargeting.

Summing up the core activity may be defined as the key activity for the achievement of enterprise focuses resp. -goals set by the person in charge. Data processing must not essentially constitute the core activity. In the end it leads to a delineation between a simply parenthetic processing and one which constitutes an inseparable part for the achievement of goals.

1.2 Who may be appointed data protection officer

According to Art 27 Para 5 DSGVO the data protection officer is appointed on the basis of his/her professional qualification and in particular of the expertise he/she has in the field of data protection law and the data protection practice, as well as on the basis of his/her capacity to perform the tasks stated in Art 39 DSGVO.

The data protection officer has to dispose of sufficient expertise and enough professional practice in data protection right and in the data protection practice. These requirements can only be met by persons who have proficiency in the fields of law, organization and technics. Besides, social skills are an essential factor for exercising the duty of data protection officer. The data protection officer should also be able to prove professional practice in one of the abovementioned fields (law, organization, technics). The required level of expertise should be particularly oriented on the performed data protection procedures and the necessary protection for the personal data processed by the person in charge or by the data processing company.

Within the scope of the law a data protection officer should be able to competently cover at least the following legal matters:

- Civil rights, particularly Art 8 EMRK (European Convention on Human Rights) and Art 7 and 8 GRC (Civil Rights Charter)
- EU Data Protection Basic Regulation
- Data Protection Act 2018
- Planned E-Privacy-Regulation
- Telecommunication Act 2003, in particular §§ 92 through 107 TKG 2003
- Legal bases for data processing, storage- and deletion periods
- Specific legal provisions regarding data protection (for example Health Telematics Act, Health Telematics Regulation)
- Labour constitution Act, in particular §§ 91, 96, 96a and 97 ArbVG
- Contract law

Within the scope of technics, the data protection officer should at least have the following basic knowledge:

- Operating modes of modern information- and communication technologies (Internet, E-Mail, Over-The-Top communication services, Cloud-services)

- Security risks, in particular 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

Within the scope of organization, the data protection officer should be familiar with the following disciplines of the Management-doctrine:

- Audit technique
- On-the-job training resp. building of awareness
- Project- and process management

The data protection officer should furthermore have a good view of his/her organization and dispose of extensive knowledge regarding the core business and the core processes. That should make it significantly easier for the data protection officer to get access to the relevant data processing procedures within his/her organization and to do counselling in respective questions at an early stage.

The stated requirements for future data protection officers are highly demanding. The data protection officer has to dispose of extensive knowledge in complex fields. Regular attendance of further training within the next few years will be indispensable for nearly every data protection officer. Lawyers and jurists will need to catch up in the fields of technics and organization. Data protection officers with a different educational background will have to expand their (data protection) legal knowledge. The necessary resources shall be made available to the data protection officer by the organisations.

The data protection officer has to perform important "translation work". Because he/she will be confronted with technical, legal and organizational problems. At this point it is therefore clearly recommended that enterprises also facilitate further trainings for the data protection officer within the scope of social skills (communication- and conflict solving capacity as well as presentation- and mediation techniques).
Such further trainings, which are financed resp. facilitated by the enterprises, may generally not be - as is common practice - bound to whatever binding obligations or repayment obligations for the data protection officer. This contradicts the independence and freedom from instructions to be warranted.

1.3 Constellation person in charge/data processing company and groups of enterprises:

If data processing is made within a relation to a data processing company, the person in charge and the data processing company should ponder - on the basis of the specified criteria - whether the appointment of a data protection officer is required with both of them or whether only one of them is obligated thereto. It is recommendable to establish a clear situation by contract. In this respect it shall be particularly considered where and how the data are actually being processed as well as who carries the actual risk of the data processing.

According to Art 37 para 2 DSGVO a group of companies may appoint one common data protection officer, if he/she is easily reachable from every location. A group of companies consists of one controlling company and other enterprises independent from the controlling one, when the controlling company is entitled to have data protection rules implemented (see Art 4 sub-para 19 DSGVO cons. reason 37). In which cases a controlling position of an enterprise is given, is an issue of corporate law and is therefore subject to the respective national law, when for Austria the relevant corporate law provisions inclusive of jurisprudence, are in particular § 244 UGB (Austrian Commercial Code) and § 15 AktG (Austrian Stock Corporate Act).

The goal of common data protection officers is also the possibility to easily contact him/her and claim his/her counselling. Criteria for the cited reachability are therefore physical and medial availability as well as the non-existence of language barriers. In international groups of companies, a complete centralization of tasks will be difficult to achieve due to the last-mentioned criterion, because the availability for customers is particularly missing in all the languages of those countries where the group has locations, and the communication of the data protection officer with the competent authority will hardly be possible in the official language of each country.

Authorities and official bodies may also appoint a common data protection officer. The criterion is here that the size and organizational structure of these authorities, resp. official bodies needs to be considered. This indicates that particularly an equal portfolio of tasks assigned by statutory law shall foster such common appointment, as it is the case for example with communities, district commissions or smaller county courts.

The wording of Art 37 para 2 DSGVO indicates that vis-à-vis the controlling authority the required appointment of the data protection officer by the controlling company of the group is sufficient.

The data protection officer may either be appointed from the pool of own employees (internal data protection officer) or an external person resp. an external company may be entrusted with this role (external data protection officer). All persons of such an external company entrusted with the tasks of the data protection officer, shall meet the requirements of the DSGVO (e.g. none of these persons may be subject to a conflict of interest with other duties). Reciprocally, all these persons must be protected to the same extent by the DSGVO (e.g. no termination of the order agreement because of the activity as data protection officer). With regard to legal security and good organization it is recommended to assign the tasks within such teams of data protection officers, being able to work together more efficiently due to different skills and strengths, in a clear way (e.g. contractually or by guidelines) and to determine one person as the main contact person, resp. the competent person for each request (Guidelines on Data Protection Officers, P. 12). Within the scope of his/her activity the data protection officer will himself/herself have access to personal data of the respective principal (see Art. 38 para 2 DSGVO). It remains open whether thereby an additional data processing relationship is being established - with all the consequences (Conclusion of a data processing contract etc.). This would not be compliant with the freedom from instructions and the independence of the (external) data protection officer.

A common data protection officer for persons in charge and data processing companies is also imaginable, but he/she will come to his/her limits of conflicts of interest where the counselling- and

controlling activity is aggravated or made impossible by different interest situations (e.g. in the assessment of risks of a project). Such constellations therefore have to be decided in each individual case taking into consideration the potential conflicts of interest.

1.4 How is the appointment of the data protection officer made?

It is anyhow recommended to make a written appointment. You will find a template for the appointment of a data protection officer in attachment 1 to this document.

The contact data of the data protection officer shall be published and noticed to the controlling authority. For publishing purposes, it is best to state the contact data on the company website, resp. for employees on the Intranet. It is not absolutely necessary to state personal phone numbers or E-Mail-addresses of the data protection officer. It shall be secured that persons concerned can easily reach the data protection officer and enter a dialogue with him/her via the stated contact data (general phone number, general E-Mail-address of the data protection officer, such as for example datenschutzbeauftragte/r@xvzat).
The data protection officer shall be noticed by name to the data protection authority. Upon consultation the Austrian Data protection authority requires a short information on the name of the company and the name of the appointed person, when an informal information via E-Mail to the data protection authority (dsb@dsb.at) is enough.

1.5 Integration of the data protection officer in the company organization

The DSGVO allows the appointment of an internal employee as well as an external service provider (Art 37 para 6 DSGVO). In practice it shall however be secured that the data protection officer may perform his/her task most effectively. It may be absolutely useful to split the tasks of the data protection officer between several persons. A thinkable option would be the appointment of an external data protection officer together with the nomination of an internal contact person, who then jointly address and administer the data protection issue within the company. The combination of internal and external experts can have absolutely positive side effects, such as by the combination of deeper knowledge of the organization from the inside with the objective view from the outside. External service providers servicing several data processing responsible persons and/or data processing companies, may in turn place their experiences with different industries and enterprises in the work with the individual person in charge. Even without the involvement of external counsellors the splitting of tasks may be usefully established, when e.g. a board of experts from various company departments, with various tasks within the company (compliance, information security, human resources management, works council etc.) is established for the support of the data protection officer.

2 Position of the data protection officer

The data protection officer is a key figure for the successful implementation of the requirements of the DSGVO in Europe. The DSGVO insofar concedes appropriate specialities to the data protection

officer, if the position within the organization structure and the inclusion in entrepreneurial decisions is concerned, which in some way or the other might be connected to the protection of personal data. The data protection officer shall be involved at an early stage and the organization shall secure his/her independence and freedom from instructions (see Art. 39 DSGVO).

2.1 Independence and freedom from instructions

According to Art 38 sub-para 3 DSGVO the data protection officer is free from instructions with regard to the fulfilling of his/her duties and may not be dismissed or disadvantaged because of reasons which arise in connection with the fulfilling of his/her duties. These privileges shall ensure that the data protection officer may perform his/her tasks without influencing. It is herewith not of importance whether the appointment of the data protection officer is made voluntarily or by obligation. For companies therefrom results the necessity to thoroughly examine a possible external or internal data protection officer before he/she is entrusted with this task. In order to be able as a company to react to changes in the company environment despite being committed to a data protection officer, it is recommended to limit the appointment of the data protection officer to a certain period. Jurisprudence up to date in countries where compulsory data protection officers already exist, particularly Germany, however requires a minimum period, enabling the data protection officer to usefully meet his/her duties. With regard to internal data protection officers a period of two to five years is herewith regarded sufficient. With regard to external data protection officers a first contract with a duration of one to two years is recommended and later contracts with a duration of four years. A shorter limitation in terms of a probation time has not been acknowledged. The thorough examination of suitability shall therefore take place before appointing.

2.2 Instruction freedom

Implications of Labour Law

The employer has a basic instruction right vis-à-vis the employee. This is a core element of employment relationships and the last level within the labour-law-related hierarchical structure.
This serves amongst others the ascertainment of employment relations such as working time, work place and the content of activities to be carried out. Furthermore, regulations concerning overtime, division of working time, break rules, holidays, annual closings, quality of the work, order behaviour (e.g. smoking prohibition or type of clothing) etc. belong here.
The employee may refuse compliance with an order if it infringes a law or if he/she is being harassed in any other way. To date excluded from instructions in the Austrian Labour Law are security confidants, works council, executive board and management.
The instruction right within judiciary bodies on the other hand is stipulated in detail in the law; Instructions of the Senior prosecution authority and of the Federal Minister of Justice may be issued in writing only and inclusive of a justification.

Implications of Data Protection Law

Art 38 para 3 DSGVO stipulates the instruction right vis-à-vis a data protection officer. The person in charge shall ensure that the data protection officer remains free from instructions in the

performance of his/her duties. The internal data protection officer is thereby only free from instructions by the employer within the scope of data protection. All other instructions beyond this connection (working time and -place, holidays etc.), are not included.
The Art-29-Data Protection Group does not issue any general recommendation on how the freedom from instructions of the data protection officer shall basically be handled, but it does however give some precise advice.
Art 38 DSGVO together with ErwGr (consideration reason) 97 provides that the freedom from instructions deliberately only exists for the scope of the data protection officer.

This means that only where the performance of duties in the capacity of data protection officer is concerned, no instructions may be issued. Particularly on page 15 of the Guideline on Data Protection Officers of the Art-29-Data Protection Group it is indicated that the data protection officer may not be directed to how he/she should initiate an examination in a complaint procedure, or how and when he/she should contact the controlling authority. That is at the sole discretion of the data protection officer. Furthermore, a data protection officer may not be instructed on how to interpret data protection rules or which judgement he/she should come to.

The person in charge therefore always remains responsible for the compliance with data protection laws and -regulations. If decisions of the person in charge are not in line with data protection laws, the data protection officer must have access to the highest management level to be able to explain his/her opinion and evaluation.

3 Organizational positioning of the data protection officer and potential conflicts of interest

The data protection officer may, beside his/her own activities, equally adopt other duties. Thereby attention shall be paid to the fact that these duties do not lead to a conflict of interest.[6] The data protection officer shall be independent and free from instructions. He/she monitors the compliance with data protection rules within the company or the authority. If assigned duties constitute a conflict of interest with the activity as data protection officer, this contradicts his/her independent position. It may not lead to the situation that the data protection officer has to control him-/herself.
With the assignment of duties, it shall also be observed that enough time remains for the data protection officer to perform his/her duties and that he/she is provided sufficient resources for a reasonable performance of his/her tasks.

- Conflicts of interest may[7] particularly exist in the following cases:
  - Management of authorities and enterprises
  - Management IT
  - Management HR
  - Management Legal
  - Management Marketing

[6] Art 38 para 6 DSGVO
[7] We identify potential conflicts of interest which shall be examined and evaluated in each individual case and which depending on the respective result either exist or not.

- Investigation bodies such as compliance officer or internal revision: If these are instructed with the performance of precise controlling measures, that may lead to conflicts of interest. To meet their examination tasks, investigation bodies are interested in a most unlimited access to data and data processing. This is the case for example when the internal revision institution within the scope of their activity requires extensive analyses of personal data or record data. With the evaluation whether there is a conflict of interest with investigation bodies, it shall also be considered whether this activity is free from instructions or not.
- Employees if they may determine or substantially influence data processing procedures (e.g. within the IT department or in the human resources department).
- Organization units with specifically extensive processing of personal data or with the processing of specific categories of personal data according to Art. 9 DSGVO (e.g. competence for Big-Data-applications)
- Works council: with regard to the works council it is controversial whether a conflict of interest exists. In this respect this shall be thoroughly pondered. There is the danger that decisions are taken according to labour law provisions and that that leads to a conflict of interest with data protection. According to the DSGVO the data protection officer shall be involved by the person in charge or by the data processing company at a most early stage. In case of the works council it is not guaranteed that it receives all information regarding the processing of employees' data at an early stage. Moreover, the role of the works council consists of representing all employees, the data protection officer shall also represent the interests of enterprises and of other concerned persons.

Furthermore, it is reasonable to document where conflicts of interest exist. It should also be stated how much time is absorbed by the activity as data protection officer. These parameters shall be appropriately considered with the occupation of the position.

3.1 Necessary resource facilities of the data protection officer

The person in charge and the data processing company are obligated to support the data protection officer in the performance of his/her duties listed in Art 39 DSGVO, in the way that they provide him/her with the resources necessary for the performance of these duties as well as access to all relevant information. It is therefore anyhow inadmissible not to involve the data protection officer or only selectively in planned data use, for the purpose of preventing uncomfortable recommendations. At the same time this is not practicable and would in a way reduce the position of the data protection officer to the absurd.

Resources which have to be provided also include employees, budget, premises. There are no general rules neither for the number of employees nor for the level of budget - in practice the company business and the number and complexity of the questions will be decisive in each individual case.

The following aspect may however be considered with regard to big enterprises: The German Federal Commissioner for Data Protection and Information Freedom recommends the complete release of one person for official bodies with 1000 employees onwards. For small and medium-size enterprises, single businesses, resp. start-ups for services of the information society this number

shall not be decisive. Here it shall on the other hand be evaluated to assign to the designated data protection officer who is not fully used to capacity, with further tasks which are not incompatible.

Beside human resources the Art-29-Data protection group states the following issues as central in the Guidelines on Data Protection Officers, P 13f:

- Active support of the data protection officer by the managers of the organization (e.g. the board of directors)
- Support in the form of a budget and infrastructure (office rooms resp. facilities)
- Announcing of the appointment and the contact details of the data protection officer to all employees, to publicize his/her existence and role
- Access to other company departments such as human resources, Legal, IT, information security etc., to provide the necessary support and information to the data protection officer
- Continuous training, especially with regard to the developments within the scope of data protection (e.g. via seminars, interest groups, workshops etc.)

The more complex, resp. sensitive the data processing of an organization is, the more resources shall be provided to the data protection officer. The data protection function must be efficiently and sufficiently equipped in relation of the data processing and the accompanying risk for the persons concerned.

With regard to the resources for maintenance of expertise there do not exist any detailed specifications either - very much here equally depends on company practice in the end. This will however only apply for internal data protection officers who are appointed from inside the organization or the group of companies and not for external service providers. The (not resolved) draft for the amendment to the Austrian DSG 2000 (Data Protection Act) as of 2012 (§ 17a para 8 of the draft of a DSG-Amendment 2012) provided for the data protection officer the offering of a training of 40 hours, to the extent of 20 hours in each following year. These thoughts may of course also in terms of the DSGVO serve as - non-committal - backup for the practical organization.

3.2 Responsibility of the data protection officer

The data protection officer is designed as counselling institution in all questions of data protection. Beside the tasks stated in Art 39 DSGVO, the data protection officer may also assume further tasks if that does not lead to incompatibilities.
If these "further tasks" consisted of management tasks in connection to the use of personal data, the data protection officer would be put in the situation of having to counsel him-/herself, what would conflict with the concept of an independent data protection officer equipped with institutional guarantees.

This means that the data protection officer may never make decisions on how personal data are used (inclusive of the group internal specifications thereto) and that a respective decision-making power will automatically lead to a conflict of interest between the "counsellor" and the "decision-maker".

This means further that the data protection officer may never be appointed „person in charge" according to § 9 Vests (Austrian Administrative Penal Act), as far as violations of data protection law are concerned, because the statutory requirement therefore would be the „respective authority to exercise command", which would have enabled the appointed person to prevent the violation against administrative criminal law (here data protection law).[8] This however blatantly contradicts the role of the data protection officer.

Responsible for the compliance with the DSGVO is the person in charge, resp. the data processing company. Only they can be addressee of penalties/fines according to 83ff DSGVO.[9]

The data protection officer therefore exclusively has the following tasks:

- Contact tasks: The data protection officer is the first point of contact for the data protection authority in all questions of data processing by the organization and closely works together with this authority
- Counselling tasks: Here the counselling of the management (board) is meant, of employees and also of concerned persons who address the data protection officer
- Training tasks: The data protection officer is responsible for the training of employees and of the management
- Control tasks: The data protection officer is responsible for the monitoring of compliance with the DSGVO and other data protection rules as well as of the strategies of the person in charge or the data processing company regarding the compliance with the DSGVO. The data protection officer shall be involved with the performance of data protection-consequences assessments and shall report to the top management on a regular basis.

4 Differentiation of the tasks of the data protection officer from other positions within the organization

We recommend a clear description of tasks of the data protection officer. The tasks which a data protection officer has to perform within the scope of a data protection organization, per se overlap with the already known roles in an organization, such as e.g. compliance and information security. The Art-29-Data Protection Group[10] even demands basic knowledge of the data protection offices in these fields. To prevent negative as well as positive conflicts of competence, the tasks of these functions should be described in detail and assigned to the respective responsible persons within an organization. A cooperation with these persons is anyhow recommendable in practice.

5 Position of the data protection officer with regard to labour law

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

[9] See Art 5 para 2 DSGVO: "The person in charge is responsible for the compliance with paragraph 1 and shall be able to prove compliance with it ("Accountability")." Equally Art 24 in connection with EG 74, DSGVO.

[10] http://ec.europa.eu/newsroom/document.cfm?doc_id=43823

The legislative body did not provide any rules regarding the exceptional position of the data protection officer in the Data Protection-Amendment 2018[11] . On the basis of the specifications in Art 38 para 6 DSGVO it shall however be assumed that the data protection officer is granted a so-called protection against dismissal on motive, as the Austrian law also provides in other cases: In these cases, there is a statutory specific protection against dismissal for certain persons[12]. With regard to these employees a dismissal is only allowed upon consent of the court/ federal social security authority. There is no such stipulation for data protection officers. To put data protection officers in the same legal position with regard to sacking and dismissal protection, an explicit statutory stipulation would however be required. Such is missing. The position of the data protection officer may most likely be compared to the position of security confidant[13]. This person is equally free from instructions as per statutory law. If a security confidant is given notice or dismissed, he/she may appeal against the notice of termination or dismissal in court, if it has happened because of his/her activity for the security and health protection of employees. It is questionable whether a data protection officer will be able to refer to the same legal protection without a statutory basis. We suppose that Art 38 para 6 DSGVO will only be able to unfold its full direct effect if the data protection officer is actually granted this position regarding termination- and dismissal scenarios. Insofar the fired/dismissed data protection officer should be entitled to appeal in court against a dismissal/notice executed unlawfully.

External data protection officers

The opinion of the Art-29-Data Protection Group may not be neglected, which extends the special dismissal protection also to the relation between principal and external data protection officer on the basis of a service agreement. Even if it is questionable whether this will in practice be confirmed by the competent courts, it is legally stringent that the DSGVO itself does not make any distinction with the stipulation of Art 38 para 3 DSGVO. To prevent unnecessary contractual obligations' conflicts, it is recommendable especially with external data protection officers to provide a limited appointment (see also item 2.1).

6 Tasks of the data protection officer

6.1 Contact tasks

The data protection officer is the main contact person for the data protection- resp. the controlling authority. Here special attention will have to be paid to the fact how the data protection officer presents him-/herself vis-à-vis the data protection authority, when he/she has to be careful to actually only assume a coordination- and platform role and not to act beyond as a "representative" of the organization of the person in charge. The latter would collide with the position of the data protection officer as an independent and instruction-free counselling office. The data protection

[11] BGBl (Federal Law Gazette) I 2017/120.

[12] Specific dismissal protection is granted to future mums as well as mothers and fathers who are on parental leave or doing a part-time job due to the birth of a child (parental part time), members of the works council or coequal persons, recruits and conscientious objectors performing community service as well as women in training service, advantaged disabled persons and victims' welfare recipients as well as janitors.

[13] Regulation of the Federal Minister of Labour and Social Affairs on the security confidants (SVP-VO) StF: BGBl. (Federal Law Gazette) Nr. 172/1996, amended by BGBl. II Nr. 324/2014

officer is therefore wisely advised to clearly communicate personal legal opinions or views of facts as such and not to leave the impression of wishing to express or represent opinions of the enterprise. At the same time, he/she should regularly internally discuss and agree, in order not to torpedo strategic considerations.

6.2 Counselling-, monitoring-, and training functions

The data protection officer furthermore has a counselling-, monitoring-, and training function within the company:

Counselling

The data protection officer informs and thereby counsels

- the management,
- the employees engaged in the processing of personal data
- all employees as persons concerned
- the works council (if existing) e.g. with respective company agreements
- upon request the responsible people with the performance of the data protection-consequences assessment.

Monitoring

The data protection officer monitors the compliance with all data protection rules, such as

- DSGVO
- Other data protection rules in the EU (e.g. Data Protection Regulation for electronic communication)
- National laws (e.g. Data Protection Act, Telecommunication Act, Labour Constitution Act, E-Commerce Act, Health Telematics Act etc.)

This monitoring obligation concerns the examination of the relevant processes and procedures for the performance of the requirements of the DSGVO, such as

- processes for the exercise of rights of concerned persons
- the process for the information of the public and the concerned persons
- development processes (data protection by design)
- examination of the admissibility of processing with new software to be implemented

This monitoring obligation also concerns the examination of the requested documents and agreements, such as

- procedure index
- data processing agreements
- EU standard agreement clauses with data transfer to third party countries
- data protection declarations and legally effective acceptance declarations
- commitment of employees for compliance with data protection
- internal guidelines for the handling of IT Assets

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

The monitoring activity will be best performed by a data protection audit to be made by the data protection officer on at least a yearly basis irrespective of the size of the company. The result of the audit shall be reported to the management and shall contain proposals for measures to be performed due to the deviations found.

Active activity

With the elaboration and possibly also with the performance of awareness trainings the data protection officer shall actively cooperate.[15]

Cooperation with the controlling authority; contact person for the controlling authority.

7 Data protection officers in authorities and official bodies

The statements in the present document essentially also apply to the appointment, position and duties of data protection officers in official bodies. The DSG Amendment Act 2018 provides some few particularities for "official" data protection officers: They are explicitly declared free from instructions and shall exercise their duty independently (§ 5 para 2 DSG). Within the sphere of ministries and downstream offices data protection officers shall be recruited from these institutions, the appointment of other, also of external data protection officers is anyhow inadmissible.[16] Finally the data protection officers in the public sector are by law in § 5 Abs 3 DSG assigned to maintain a regular exchange of experience with regard to the warranty of a uniform data protection standard.[17]

The data protection officers in the public sector have a seat in the Data Protection Council (§ 21 para 6 DSG).

Data Protection officers shall report to the top management. In the public sector it can be assumed that this will be the minister him-/herself or the comparable top-level body in an administrative organization (Federal authorities, state authorities, communities).

---

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

[15] Remark: These procedures and documents rarely exist with medium-sized and smaller enterprises. Here the data protection officer will reasonably cooperate with the establishment of the documents.

[16] Even if this matches the opinion of the Art-29-Data Protection Group in its regulation to the data protection officer, according to which a data protection officer in authorities and official bodies should also dispose of appropriate knowledge of administrative procedures and processes within the administration, we do not see any reason why data protection officers should be excluded here by law. The latter might equally dispose of such knowledge and experience.

[17] Here we would like to point to the regular networking meetings and internal Association seminars of Privacyofficers.at.

Sample template for the designation of a person as data protection officer according to article 37 DSGVO in connection with § 5 DSG

Designation to data protection officer according to article 37 para 1 DSGVO in connection with § 5 DSG Data Protection Basic Regulation (EU 2016/679).

Mr./Mrs. [*insert name*] _____ shall with effect as of [*Date*] be appointed as data protection officer in terms of Article 37 ff DSGVO.

The designation refers to the company/the organization/the authority [*insert name*].

The designation shall be made for an indefinite period of time/shall be limited until [*insert date*].

The designation of data protection officer may be revoked at any time for important reasons or upon request by the controlling authority. The designation shall anyhow end upon termination of the (employment) contract concluded between Mr./Mrs. [*insert name*] and [*insert name of employer*] at the latest.
It may be pointed to the secrecy obligation (notwithstanding other confidentiality obligations) as well as to the right to refuse to give evidence with the performance of your duties according to § 5 DSG.

[Signature Management]

I herewith accept my designation to data protection officer in accordance with the abovementioned content.
I herewith acknowledge that according to Art 37 para 7 DSGVO the contact details of the data protection officer (E-Mail-address, phone number and address) have to be published by the employer and that these will also have to be noticed to the data protection authority.

Place, Date
[Signature Data protection officer]