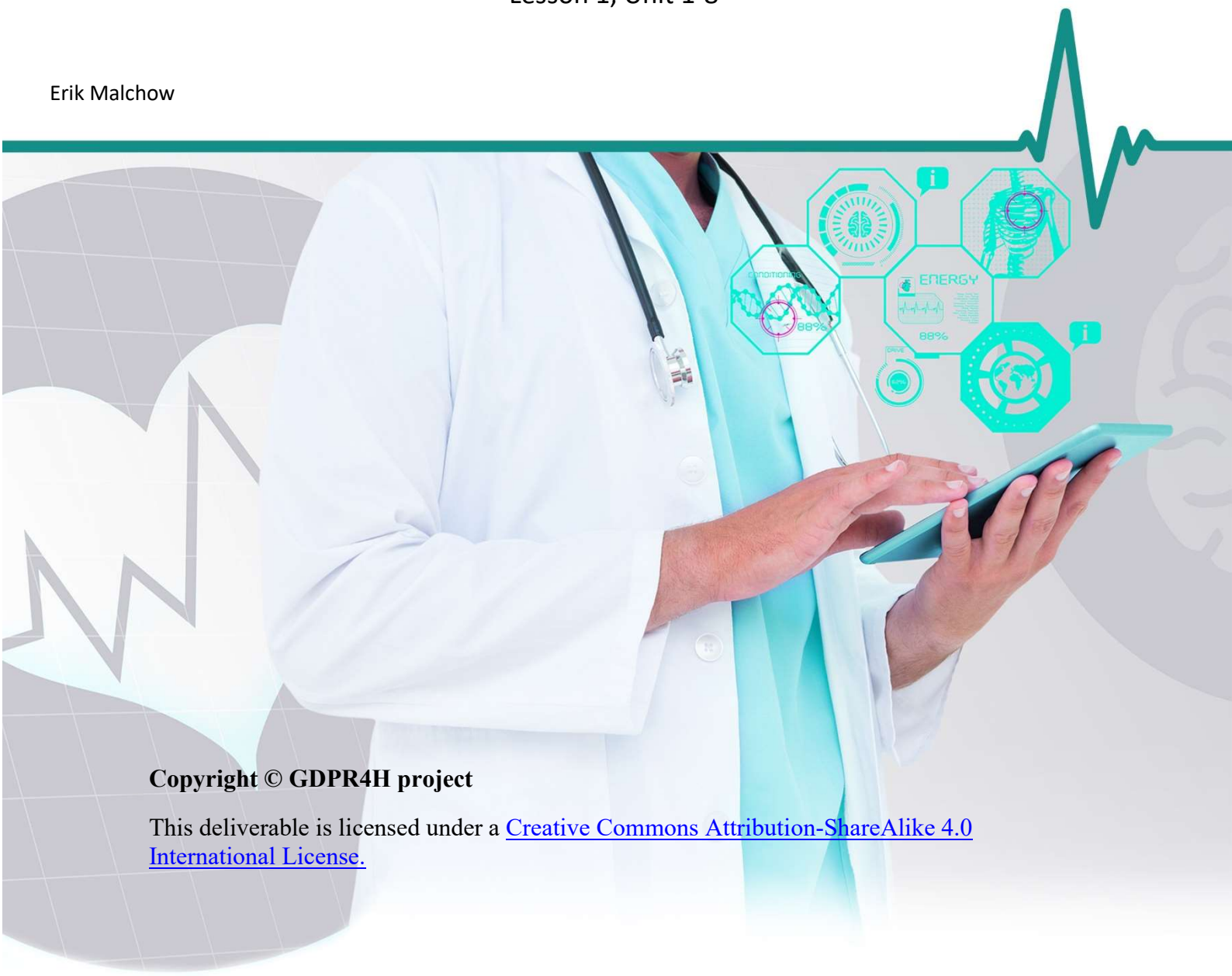
Module 3:
Soft Skills for Data Protection Officers

Lesson 1, Unit 1-8

Erik Malchow



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Framework paradigms for the DPO

The regulation mandates the appointment of a DPO in many cases, and prescribes the particular tasks and responsibilities of the DPO. This is in contrast to the current position; under most existing national laws, the appointment of a DPO remains optional.

There is a clear indication that, despite a lack of legal compulsion, a great majority of organisations view the DPO appointment as a prerequisite for corporate accountability, a matter of good corporate practice and as enabling a proactive, rather than reactive, management of data privacy within the organisation.

The Regulation sets out the tasks and responsibilities of the DPO[1], including: providing information and advice, overseeing and monitoring data protection; maintaining documentation; dealing with data subjects directly; and, consulting and cooperating with regulators. Specific tasks include developing staff training, conducting audits, monitoring the implementation of data protection by design and default, monitoring data protection impact assessments, and ensuring data security.

In a survey by the Centre of information policy leadership[2], DPOs were asked to indicate what their role entails currently, in order to understand how similar, or dissimilar, their existing role is compared to the role envisaged under the Regulation. It appears that the majority of DPOs who contributed to the survey are focused on these requirements already. The survey reveals that 87.5% of respondents advise their organisation on compliance with applicable data protection laws and internal procedure, 77.5% advise on the data protection provisions of third-party contracts, and 82.5% monitor legal and policy developments. A high proportion already oversee and monitor data protection compliance: 82.5% provide oversight of the organisation's privacy programme, 70% conduct privacy impact risk assessments, and 65% conduct compliance assessments. 82.5% already develop training and awareness tools and 85% work with the business to build data protection into the design of systems, projects, products and services. 65% already respond to data subject access requests and 67.5% deal with data subject complaints. 72.5% maintain relationships with, or act as a contact point for, the local data protection authority. On the data security front, 70% lead on data breach responses and 85% provide expert advice following a breach.

The survey appears to indicate that of all the tasks enumerated in the survey, very few DPOs actually perform the operational tasks (such as responding to and dealing with data subjects' requests and individuals' complaints, conducting assessments and verifying compliance). This is likely due to the fact that many DPOs have teams and delegate operational tasks to junior team members. Assessing and verifying compliance may be performed by other corporate functions, such as internal audit or dedicated compliance assessment teams, and not exclusively by the DPO. As some respondents indicated in their comments, there may be a conflict where a single DPO or DPO team perform both the oversight and advisory roles, on the one hand, and compliance verification and assessment roles, on the other.

[1] Article 37, Regulation.

[2] https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/role_and_function_of_a_dpo_in_practice_report_on_survey_results.pdf

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Finally, the scope of the DPO role appears to have transformed and developed over time to include public policy and external representation with regulators, industry and the media. One respondent remarked that "When [the] position [was] initially created [in 1997], it did not include a public policy component but the role now includes public policy and representing the company externally."

CEDPO adds:

> *The DPO has to face a number of challenges and with different interests at stake. That is why the DPO should also show strong communication skills combined with refined diplomacy. A DPO is not (and should not be) a "privacy activist": with the support of the other leaders of the organisation, he/she must play a role of a responsible business-enabler and help the organisation to include privacy in the business-decision processes, to not only detect and prevent risks but also create value. In addition, the GDPR requires that his/her reporting line is to the highest level of the management, and that his/her independence is ensured. This requires "gravity" and leadership skills as well.*[3]

[3] CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations, p. 3.

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Communicating duties of the DPO

In practice the tasks and responsibilities of the DPO may be fulfilled by a team of individuals. Nearly half (47%) of survey respondents indicated that they have five or more team members under their direct supervision assisting them in their role as DPO, with 15% having between 10-20 team members. It therefore appears that the tasks of the DPO are not performed by a single person, but by the privacy function within the organisation. Currently, the Regulation does not reflect this possibility.

The diverse structure and composition of current privacy functions reflects the wide range of responsibilities that commonly fall within the DPO role today. A privacy team, rather than an individual, fulfilling the role of DPO may be the best way to staff such a multi-faceted role. The DPO role requires a diverse skill set including technical and legal knowledge, commercial awareness, a deep understanding of the business, and strong communication and public relations skills. To some extent, the DPO needs to be detail-orientated, understanding the technical aspects of data processing activities and relevant technologies, and how the legal framework and IT security considerations apply. At the same time, the DPO needs to be a big picture thinker, having the vision to look around corners and the ability to view privacy issues within the wider commercial context, thereby helping the business to meet commercial objectives in a compliant manner.

Apart from resources, and a sufficiently strong, protected and senior position within the organisation, the DPO also needs to have the power the carry out his or her task. Article 38(2) makes clear that to that end the entity appointing the DPO must ensure that he or she will have “access” to personal data and processing operations. This should be read in the same way as the corresponding provision
in the regulation covering the EU institutional DPOs, Art. 24(6) of Regulation (EC) 45/2001, is read by those DPOs:

The Regulation requires controllers to assist the DPO in performing his or her duties and to give information in reply to questions, and states that the DPO shall have access at all times to the data forming the subject matter of processing operations and to all offices, data processing installations and data carriers.

Although the DPO has no enforcement power vis-à-vis controllers, he/she is empowered to monitor compliance by collecting all relevant data, which the appointing institution/body and its controllers are obliged to make available.

Other comments by the EU institutional DPOs in relation to the DPO’s duty to ensure compliance with data protection rules are also relevant:

IT tools may be developed to assist the DPO in performing regular monitoring. Administrative arrangements can also be made, such as ensuring that the DPO receives a copy of all mail raising data protection issues, and requiring that the DPO be consulted on documents raising data protection issues. Careful, regular monitoring of compliance and reporting of results can create a strong pressure on controllers to ensure that their processing operations are compliant. Regular monitoring and reporting are thus the DPO's strongest tools for ensuring compliance. To this end, an annual survey/report issued to the management is a best practice.

The European Commission’s support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Verbal strategies

Focus on the issue, not the person. Try not to take everything personally, and similarly, express your own needs and opinions in terms of the job at hand. Solve problems rather than attempt to control others. For example, rather than ignoring a student who routinely answers questions in class with inappropriate tangents, speak with the student outside of class about how this might disrupt the class and distract other students.

Be genuine rather than manipulative. Be yourself, honestly and openly. Be honest with yourself, and focus on working well with the people around you, and acting with integrity.

Empathize rather than remain detached. Although professional relationships entail some boundaries when it comes to interaction with colleagues, it is important to demonstrate sensitivity, and to really care about the people you work with. If you don't care about them, it will be difficult for them to care about you when it comes to working together.

Be flexible towards others. Allow for other points of view, and be open to other ways of doing things. Diversity brings creativity and innovation.

Value yourself and your own experiences. Be firm about your own rights and needs. Undervaluing yourself encourages others to undervalue you, too. Offer your ideas and expect to be treated well.

Use affirming responses. Respond to other in ways that acknowledge their experiences. Thank them for their input. Affirm their right to their feelings, even if you disagree. Ask questions, express positive feeling; and provide positive feedback when you can.

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Successful negotiation

Negotiating requires give and take. You should aim to create a courteous and constructive interaction that is a win-win for both parties. Ideally a successful negotiation is where you can make concessions that mean little to you, while giving something to the other party that means a lot to them.

Before entering a bargaining meeting, the skilled negotiator prepares for the meeting. Preparation includes determining goals and areas for alternatives to the stated goals. In addition, negotiators study the history of the relationship between the two parties and past negotiations to find areas of agreement and common goals. Past precedents and outcomes can set the tone for current negotiations.

Negotiators have the skills to listen actively to the other party during the debate. Active listening involves the ability to read body language as well as verbal communication. It is important to listen to the other party to find areas for compromise during the meeting. Instead of spending the bulk of the time in negotiation expounding the virtues of his viewpoint, the skilled negotiator will spend more time listening to the other party.

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Body language

Body language is a type of a nonverbal communication in which physical behaviours, as opposed to words, are used to express or convey the information. Such behaviour includes facial expressions, body posture, gestures, eye movement, touch and the use of space. Body language exists in both animals and humans, but this article focuses on interpretations of human body language. It is also known as kinesics.

Body language must not be confused with sign language, as sign languages are full languages like spoken languages and have their own complex grammar systems, as well as being able to exhibit the fundamental properties that exist in all languages. Body language, on the other hand, does not have a grammar system and must be interpreted broadly, instead of having an absolute meaning corresponding with a certain movement, so it is not a language like sign language, and is simply termed as a "language" due to popular culture.

In a society, there are agreed-upon interpretations of particular behaviour. Interpretations may vary from country to country, or culture to culture. On this note, there is controversy on whether body language is universal. Body language, a subset of nonverbal communication, complements verbal communication in social interaction. In fact, some researchers conclude that nonverbal communication accounts for the majority of information transmitted during interpersonal interactions. It helps to establish the relationship between two people and regulates interaction, but can be ambiguous.

Eye contact is important

Oculesics, a subcategory of body language, is the study of eye movement, eye behaviour, gaze, and eye-related nonverbal communication. As a social or behavioural science, oculesics is a form of nonverbal communication focusing on deriving meaning from eye behaviour. It is also crucial to note that Oculesics is culturally dependent. For example, in traditional Anglo-Saxon culture, avoiding eye contact usually portrays a lack of confidence, certainty, or truthfulness. However, in the Latino culture, direct or prolonged eye contact means that you are challenging the individual with whom you are speaking or that you have a romantic interest in the person. Also, in many Asian cultures, prolonged eye contact may be a sign of anger or aggression.

Proxemics

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Another notable area in the nonverbal world of body language is that of spatial relationships, which is also known as Proxemics. Introduced by Edward T. Hall in 1966, proxemics is the study of measurable distances between people as they interact with one another. In the book, Body Language, Julius Fast mentioned that the signals that we send or receive to others through body language are reactions to others' invasions of our personal territories, which links Proxemics an important part of Body Language.[4]

Hall also came up with four distinct zones in which most people operate:

Intimate distance for embracing, touching or whispering, Personal distance for interactions among good friends or family members, Social distance for interactions among acquaintances, Public Distance used for public speaking. In addition to physical distance, the level of intimacy between conversants can be determined by "socio-petal socio-fugal axis", or the "angle formed by the axis of the conversants' shoulders".

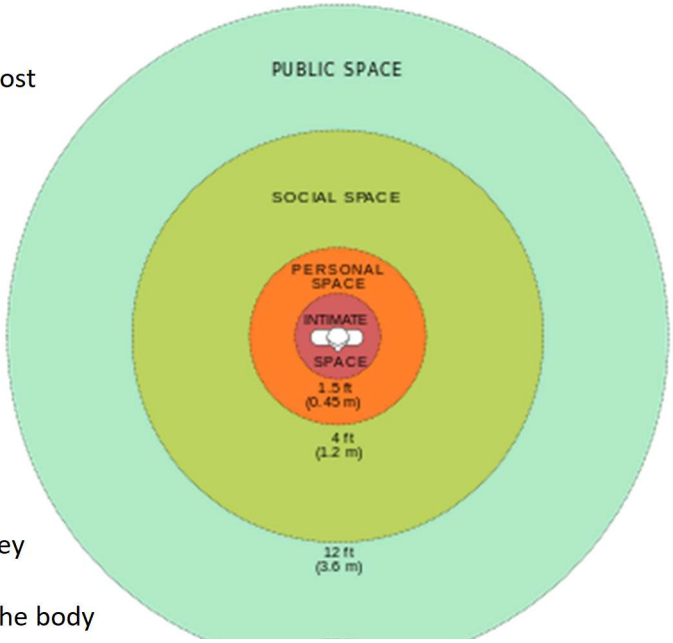


Figure 1: Proximity spaces (E.T. Hall)

Changing the distance between two people can convey a desire for intimacy, declare a lack of interest, or increase/decrease domination. It can also influence the body language that is used. For example, when people talk, they like to face each other. If forced to sit side by side, their body language will try to compensate for this lack of eye-to-eye contact by leaning in shoulder-to-shoulder.

It is important to note that as with other types of Body Language, proximity range varies with culture. Hall suggested that "physical contact between two people ... can be perfectly correct in one culture, and absolutely taboo in another".

In Latin America, people who may be complete strangers may engage in very close contact. They often greet one another by kissing on the cheeks. North Americans, on the other hand, prefer to shake hands. While they have made some physical contact with the shaking of the hand, they still maintain a certain amount of physical space between the other person.

[4] Hall

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

The position of the data protection officer in the company

According to Article 38, the controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge and the controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. 2He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. 3The data protection officer shall directly report to the highest management level of the controller or the processor. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Freedom of instruction and independence and organizational connection

The GDPR envisages that the DPO performs their work in an independent manner. In other words, the controller should not direct the DPO regarding how they do their work. For example, the DPO cannot be instructed to reach a particular conclusion concerning the investigation of a complaint. The DPO should report to the highest level of management. Ideally this should be the board of directors. This is intended to ensure compliance with the regulations in the sense that management receives timely advice on matters of data protection. The reason for this independence is in recognition of the key role that the DPO plays in ensuring compliance with the regulation.

To achieve the autonomy required by the GDPR, the DPO must be afforded some form of job security. They cannot be dismissed or penalized by the controller or processor as a result of carrying out their duties. This does not mean that the DPO enjoys permanent job security or tenure. They may be disciplined or even terminated for other legitimate reasons, such as disciplinary turpitude. Further, availing the DPO with the necessary resources is not only key to enabling them to perform their duties, but also necessary to achieve the desired independence. The scale of resources depends on the complexity and sensitivity of the processing activities but would include finances, equipment and staff.

Further, care must be taken not to compromise the autonomy of the DPO by putting them in a position that may lead to a conflict of interest. This is more likely in cases where the DPO is internal. While it is permissible to assign the DPO with other tasks, these should, for instance, not require them to determine the means and purposes of processing the data, as this would blur their role with that of the controller.

It has been accurately observed that the DPO is the manifestation of the supervisory authority in an organization. The importance of the DPO in achieving compliance with the GDPR cannot be overstated; however, the DPO is not personally liable for noncompliance, as overall responsibility lies with the data controller. Any decision not to appoint a DPO must be signed off on at a senior level in the organization. In addition, failing to appoint a DPO where one is required may attract a fine of 10 million euros or 2% of annual global turnover, whichever is higher.

To achieve the strict obligations imposed on controllers and indeed processors under the GDPR, it is important that organizations processing personal data empower and embrace their DPOs and work closely with them, as opposed to viewing them as “nosy night watchmen.”[5]

[5] Dyann Heward-Mills, CIPP/E, CIPP/US, CIPM https://iapp.org/news/a/the-dpo-must-be-independent-but-how/

The European Commission’s support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

If more than 2 answers are given, multiple answers are possible. If there are only 2 answers, only one of them is correct.

Unit 1: Communication: the relevance of the GDPR

1. The appointment of a DPO is according to the GDPR

- Optional
- Mandatory

2. What is Proxemics?

- An IT structure
- Structure of the proxy server
- Use of space
- part of body language

3. What makes more sense for an open discourse

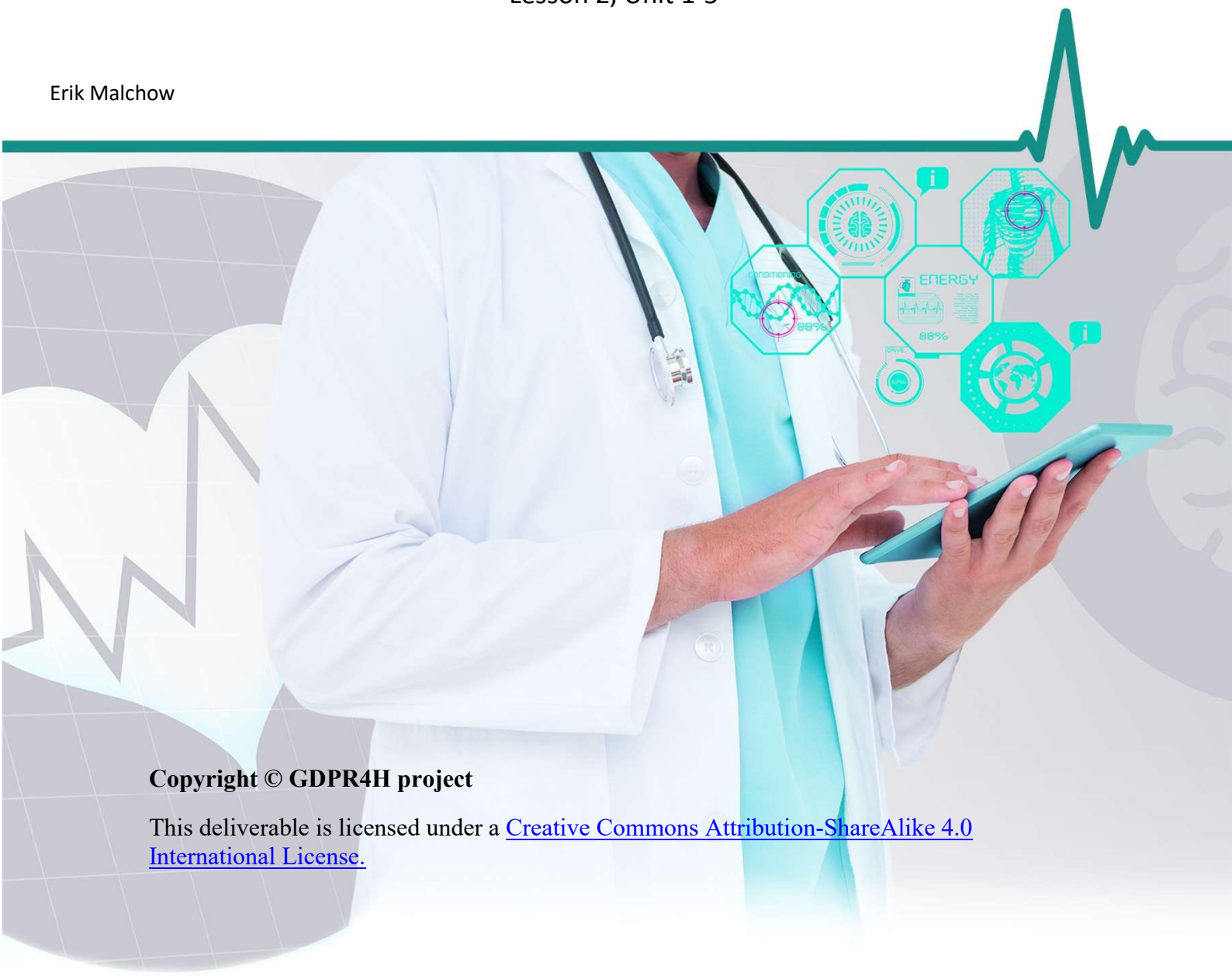
- socio-petal communication,
- socio-fugal communication

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Module 3:
Soft Skills for Data Protection Officers

Lesson 2, Unit 1-5

Erik Malchow



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Communicating Competency and Ownership

Getting the message across and to actively interfere in company culture is one of the biggest tasks for DPOs. Hence, the DPOs will explore the basics of self-presentation and Public Relations (PR) in data protection in the LO2. A competent self-representation, but also the ability to communicate responsibilities and possibilities to contact and file complaints will be taught. The participants experience and recognize which communication (in conversation, in a meeting, in a conference, with a customer, in front of their superior) are successful - clear messages, understandable language and formulations, comparisons and pictures, convincing appearance in body language and charisma.

Active interference with company culture

The hierarchical and contractual position of the DPO within an organisation is crucial in relation to ensuring the DPO's effectiveness, independence and avoidance of conflicts of interest. On the one hand, as noted earlier, the DPO should be "proximate" to the organisation he or she serves (see above, under the heading "Required expertise"). Moreover, as CEDPO puts it:

> *In order for a DPO to be effective, [she or he] should be on the ground, not only available to various stakeholders within your organization but proactively looking for opportunities to interact with different departments.*[1]

This can be problematic in cases of outside DPOs acting under a service contract: they will by definition not be part of the body they assist. In the private sector, there may well be – and in some countries, like Germany, there undoubtedly are – external DPOs with extensive expertise in the private sector or sub-sector in which they work. In the public sector, this may be more difficult (Cf. section 2.3.2, above, under the headings "DPOs for large public authorities or groups of authorities" and "External DPOs").

But there is always a tension between, on the one hand, the necessary "proximity" of the DPO to her or his organisation, and, on the other hand, the need to avoid conflicts of interest and ensure the DPO's actual independence in practice.

The issue is addressed in much more detail by the EU institutional DPOs. Although their views must of course be seen in the light of their specific context, it is still useful to note them. Having noticed various provisions in the regulation that covers them (Regulation (EC) 45/2001)290 that are designed to guarantee their independence, they continue as follows:

In practice, however, it may be challenging for the DPO to exercise his/her duties in full independence. Needless to say, the individual situation and personality of the DPO will play a role but it can generally be assumed that certain elements may tend to weaken the position of a DPO:

- A part-time DPO faces a permanent conflict between allocating time and efforts to his/her DPO tasks versus other tasks. With respect to career development and performance review, management may place greater weight on the non- DPO activities. This creates pressure on

[1] Network of Data Protection Officers of the EU Institutions and Bodies (CEDPO), Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (see footnote 244, above), p. 15.

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

the DPO to concentrate his/her efforts on the non-DPO tasks. A part-time DPO is also in danger of encountering conflicts of interest.

- The DPO with a limited contract would likely be in a weaker position to perform his/her DPO duties vigorously than one with a permanent contract (official or temporary agent with indefinite term contract). This is because he/she may be concerned about how his/her actions could negatively influence the renewal of his/her contract. A DPO who is very young and has only limited work experience may have difficulties standing up to controllers, and may be more focused on his/her own career development than on vigorous performance of DPO duties.
- A DPO who reports to, and is reviewed by, a direct superior in the hierarchy (director or head of unit) may feel pressure to cooperate and get along smoothly with management and other colleagues, as vigorous performance of DPO duties may have a negative impact on career. ... To alleviate this pressure, the DPO should report to, and be reviewed by, the administrative head of the institution or body. This is particularly important for part-time DPOs, who should report directly to, and be reviewed by, the appointing authority for their DPO duties, and to/by the normal superior in the hierarchy for other duties.
- A DPO who must request staff and resources (IT resources, budget for business trips and training) from his/her direct superior could face difficulties if the latter is not fully committed to achieving data protection compliance. This can be avoided if the DPO has his own budget responsibility, and by having any requests for additional resources subject to approval by the appointing authority.

Best practices to help ensure the independence of the DPO are:

- The institution or body should establish the DPO post within the organisation as one of Adviser, Head of Unit or Director and in any event the DPO position should be officially recognized as management level, on the official organizational chart of the institution/body;
- The institution or body should appoint the DPO for the longest term possible, in light of the DPO's contract. Thus, a five-year appointment should be the norm, unless it is not possible under the circumstances; The DPO should have a permanent/undetermined contract with the institution or body [and] should be sufficiently experienced (…);
- The DPO should be able to dedicate his/her time fully to his/her DPO duties, especially for large institutions and bodies, and for smaller ones in the initial phase of establishing a data protection regime. Proper support in terms of resources and infrastructure should be provided. The non-DPO duties of a part- time DPO should not present a conflict of interest, or even the appearance of a conflict, with the DPO duties;
- DPOs in organisations where data processing activities are the core business of the organisation will normally require various staff members. Such staff capacity should be ensured;
- Rules should be in place within the organisation ensuring the obligation of all staff members to cooperate with the DPO without having to wait for an order or permission of their superior;
- The DPO should report to the head of the institution or body, who should be responsible for review of the DPO's performance of his/her duties, as established by the Regulation. The person responsible for the DPO's performance review should be sensitive to the need for the DPO to take strong positions which others in the organization may not appreciate. The DPO should not suffer any prejudice on account of the performance of his/her duties. The appointing authority should ensure that during the DPO's term of office, he/she has at least a "normal" career advancement.

Steinbeis HOCHSCHULE ACQUIN METROPOLITAN COLLEGE CENTRE OF EXCELLENCE PEF Skybridge partners crefop arps EMA European Medical Association
Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

When reviewing the DPO's performance, the evaluator should be careful neither to reprimand the DPO for taking unpopular positions nor to consider data protection requirements as an administrative burden. For a part-time DPO, performance on the DPO duties should be given equal weighting to performance on the non-DPO duties. … ;

- The DPO should have his/her own budget line, set up in compliance with the relevant rules and procedures of the respective institution/body; his/her requests for any further resources should be subject to approval by the administrative head. Other arrangements are acceptable if they provide the DPO with the resources he/she needs to perform his/her mission in an independent manner;
- The DPO should have signing power for DP related correspondence. [2]

[2] Douwe Korff& Marie Georges The DPO Handbook
https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

spreading the word (Facebook, Instagram, Twitter, etc)

A majority of healthcare businesses have some sort of social media platform which they use to interact and engage with customers and clients – and social media is indeed a great way to connect with customers and patients. However, much like many other areas of business, data protection and compliance still applies and should be treated accordingly.

On 5th June 2018 the Court of Justice of the European Union (CJEU) passed its judgement in Case C-210/16 Wirtschaftsakademie Schleswig-Holstein. This concerned the Wirtschaftsakademie's Facebook fan page which the data protection authority of Schleswig-Holstein, Germany, sought to deactivate.

The reason for the push to deactivate the page was based on Wirtschaftsakademie's failure to warn visitors to their fan page that their personal data would be collected by cookies. In a decision that has taken much of the data protection community by surprise, the CJEU ruled that an administrator of a Facebook fan page is a joint controller alongside the social media giant itself. Although this judgement is made under the Data Protection Directive 95/46/EC, which has been replaced by the General Data Protection Regulation (GDPR), the principles on which the judgement has been based are materially the same as those of the GDPR.

The Advocate General established, in relation to Wirtschaftsakademie, sufficient control over the processing activity and the purpose of the processing activity. This essentially lead the Advocate General to disagree with the referring court's ruling that Wirtschaftsakademie is not a controller as it has no control or influence over the processing of personal data by Facebook. In fact, the case highlights two key points:

1. As well as facilitating the fulfilment of purposes for Facebook, namely enabling Facebook to target advertisements to the fan page visitors by tracking their web browsing habits, the cookies on the page fulfilled purposes for Wirtschaftsakademie by compiling viewing statistics for Wirtschaftsakademie.
2. Wirtschaftsakademie has substantial control over the processing activity as without the participation of Wirtschaftsakademie the data processing could not occur; and they could end the processing of personal data by closing the fan page down. Therefore, it was decided that the fan page owner plays an active role in determining the means and purpose of the processing of personal data.

So, what does this mean for fan page owners going forward? In summary, this judgement, if followed by the court means creators of Facebook fan pages will be as liable as Facebook for the processing of personal data in connection with their fan page.[3]

[3] How data compliance impacts social media management: A note to Facebook fan page owners https://www.dpocentre.com/how-data-compliance-impacts-social-media-management-a-note-to-facebook-fan-page-owners/

Public Relations are a must – transparency

A fundamental part of the function of public relations — particularly on the PR agency side of the fence — relies on the collection, storage and use of personal information for media relations. The ability to generate earned outcomes inevitably relies on the ability to contact journalists, analysts and influencers, which implies the creation of media lists and databases holding personal data about these individuals.

The concept of 'legitimate interests' is a useful one. Essentially it means that if an organisation can claim to need to process personal data in order to do its job, then it should be allowed to do so (though not that this negates any need for transparency in the data they capture and use, nor the ability for individuals to choose not to have their data kept and used).

A knock-on impact of GDPR for healthcare businesses should also be the promotion of good behaviour and discipline in communications, whether with third-party influencers or end customers themselves. Doctors recognise the need for PR agencies to help them do their jobs. What they react against are poorly considered pitches that don't take into account their specific areas of interest and focus, or general, scattergun approaches that border on spam. If GDPR has increased awareness of an appropriate use of personal data then again, it will have had a positive effect.

While the detail of GDPR can be seen as complex, its core principle is a simple one. If it hasn't already done so, any organisation dealing with the personal data of EU residents in any way should take appropriate advice and action to ensure compliance.

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Storytelling

Storytelling describes the social and cultural activity of sharing stories, sometimes with improvisation, theatrics, or embellishment. The term "storytelling" can refer in a narrow sense specifically to oral storytelling and also in a looser sense to techniques used in other media to unfold or disclose the narrative of a story.

In the workplace, communicating by using storytelling techniques can be a more compelling and effective route of delivering information than that of using only dry facts.

For DPOs storytelling is an important way of resolving conflicts, addressing issues and facing challenges. Managers may use narrative discourse to deal with conflicts when direct action is inadvisable or impossible. In a group discussion a process of collective narration can help to influence others and unify the group by linking the past to the future. In such discussions, the DPO can transform problems, requests and issues into stories. Jameson calls this collective group construction storybuilding.[4]

Storytelling plays an important role in reasoning processes and in convincing others. In business meetings, managers and business officials preferred stories to abstract arguments or statistical measures. When situations are complex or dense, narrative discourse helps to resolve conflicts, influences corporate decisions and stabilizes the group.[5]

[4] Jameson, p. 476 ff.

[5] Idem.

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

If more than 2 answers are given, multiple answers are possible. If there are only 2 answers, only one of them is correct.

Unit 2: Communicate competence and personal responsibility

1. Which statement is correct?

- Data protection officers must be employed in the company.
- Data protection officers must be able to act in the interest of data protection regardless of the company's interests.
- Companies can hire external, independent data protection officers.
- A data protection officer cannot be terminated.
- Employed data protection officers who also take on other tasks in the company must ensure that they do not come into any conflict of interest.

2. Conflicts of interest for employed data protection officers can arise if

- the PR department wants to use customer data for communications
- the data protection officer is privately interested in other topics
- the management does not want to report an attack on the IT system for fear of a scandal

2. Storytelling can be used by the data protection officer to ...

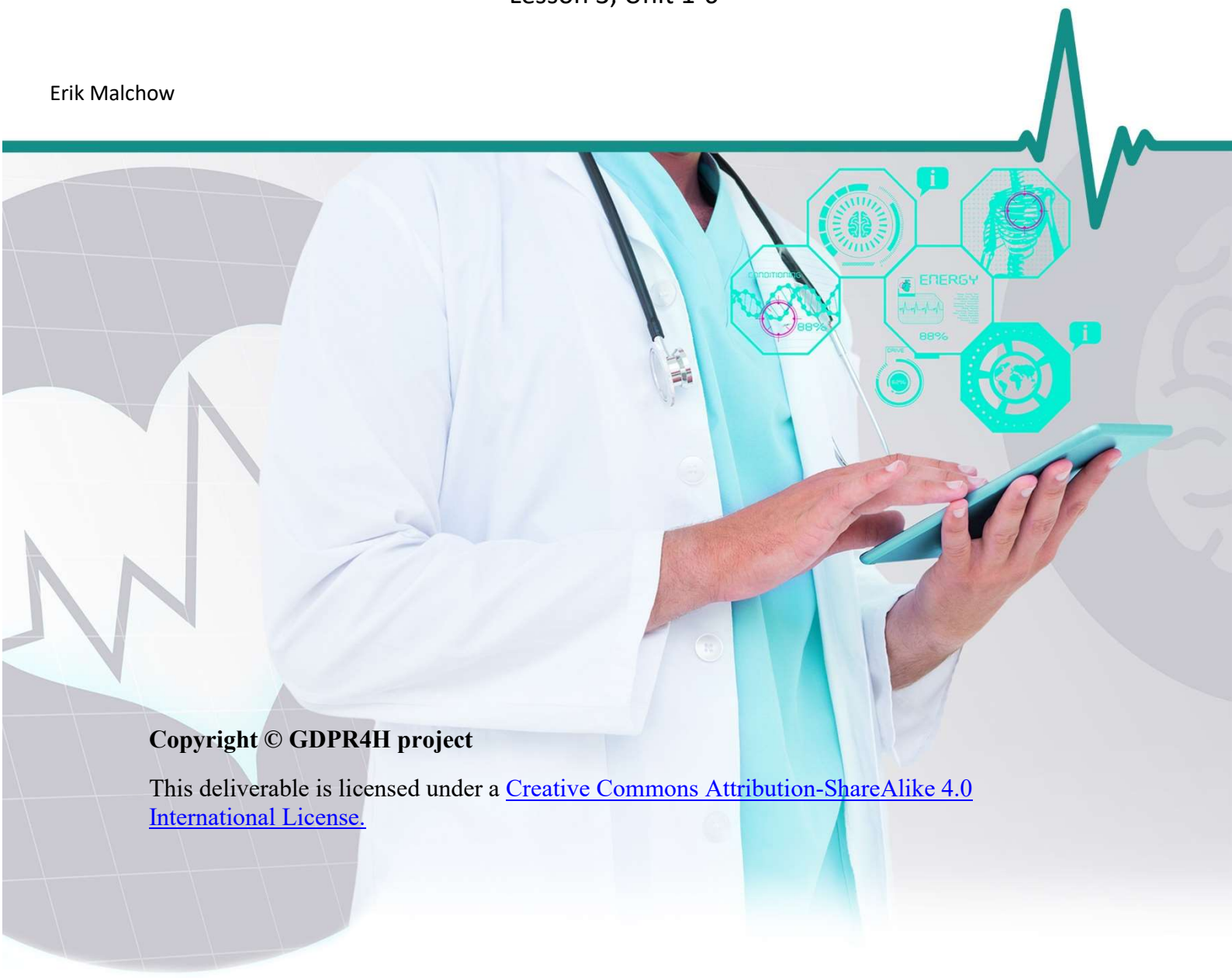
- integrate the importance of data protection into the corporate culture
- spread rumors in the departments
- to convey dry facts in an interesting way
- to appease conflicts
- objectively argue with statistics

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Module 3:
Soft Skills for Data Protection Officers

Lesson 3, Unit 1-6

Erik Malchow



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Crisis Management

A successful GDPR implementation usually creates conflict, as it interferes with company culture and demands change. The conflict that is connected to the morphology of the health institution will have to be solved in an orderly matter. Hence, a DPO is very often also responsible the handle conflicts before their escalation. The aim of the third LO is to make the DPO aware of an upcoming conflict and how to cope with conflict stages (Glasl).

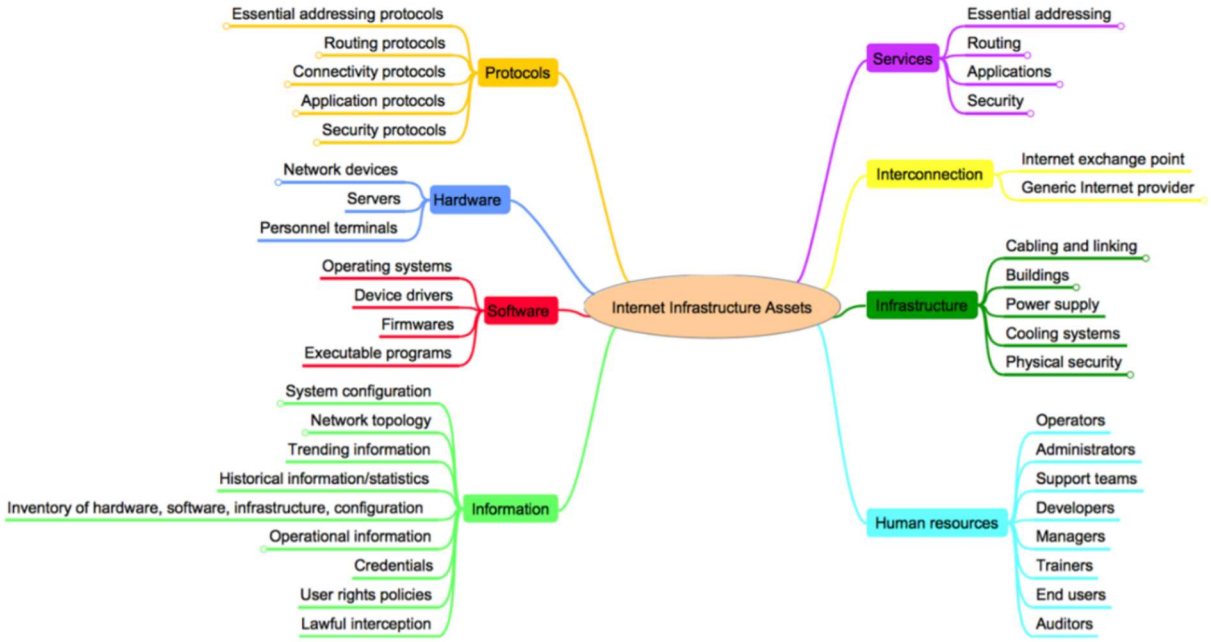


Figure 1: infrastructure assets (courtesy of ENISA)

The most common risk cases in GDPR measures derive from technical issues like “Massive unavailability of desktops“ and “Logical unavailability of Information systems” [1]. To communicate accordingly about conflicts and risks is often connected to conflicts of interest. For a CFO, revenue is essentially more important than data protection. Informing a CFO about possible fines that will eventually decrease cash flow in the company can be one way to communicate the importance of GDPR. Still there are many more polite ways to act.

How to avoid conflicts of interest

As the WP29 notes that Article 38(6) allows DPOs to ‘fulfil other tasks and duties’. It requires, however, that the organisation ensure that ‘any such tasks and duties do not result in a conflict of interests’.

The absence of conflict of interests is closely linked to the requirement to act in an independent manner. Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interests. This entails in particular that the DPO cannot hold a position within the organisation that leads him or her to determine the

[1]https://www.caceis.com/fileadmin/documents/pdf/Who-We-Are/Compliance/CACEIS_Group_Information_Security_2019v1.4.pdf

Steinbeis HOCHSCHULE ACQUIN METROPOLITAN COLLEGE CENTRE OF EXCELLENCE PEF Skybridge partners crefop arps EMA European Medical Association
Erasmus+ The European Commission’s support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.

As a rule of thumb, conflicting positions may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing.

Depending on the activities, size and structure of the organisation, it can be good practice for controllers or processors:

- to identify the positions which would be incompatible with the function of DPO
- to draw up internal rules to this effect in order to avoid conflicts of interests
- to include a more general explanation about conflicts of interests
- to declare that their DPO has no conflict of interests with regard to its function as a DPO, as a way of raising awareness of this requirement
- to include safeguards in the internal rules of the organisation and to ensure that the vacancy notice for the position of DPO or the service contract is sufficiently precise and detailed in order to avoid a conflict of interests. In this context, it should also be borne in mind that conflicts of interests may take various forms depending on whether the DPO is recruited internally or externally.

The EU institutional DPOs add:

> *[T]he DPO should not have conflicts of interest between DPO duties and any other official duties, in particular in relation to the application of the provisions of the Regulation (Art. 24.3). A conflict of interest is present when the other duties,which a DPO is asked to perform, may have directly adverse interests to that of protection of personal data within his/her institution. If necessary, the DPO should raise this matter with his/her appointing authority.*

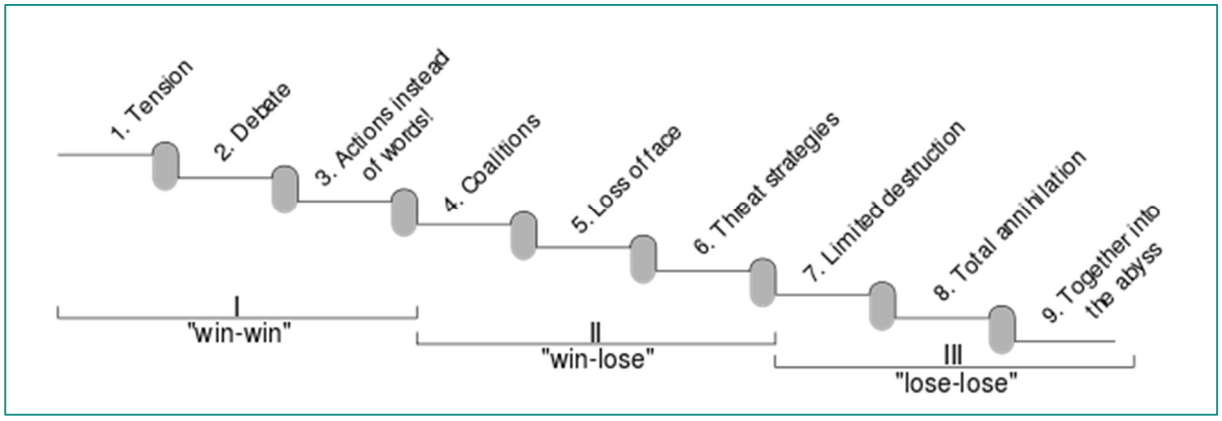
They address the issue in more detail in terms of contractual-, length of appointment and other safeguards, as noted under the next heading. CEDPO again merely notes that, if the DPO appointment is not a full-time job, the organisation that appoints her or him should "consider … how to deal [with] conflict of interest".[2]

[2] CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations (footnote 239, above), p. 3,

Steinbeis HOCHSCHULE ACQUIN METROPOLITAN COLLEGE CENTRE OF EXCELLENCE PEF Skybridge partners crefop arps EMA European Medical Association

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Glasl represents "escalation in his nine stage model not as an ascent to higher and higher stages of escalation, but as a descent to deeper and deeper, more primitive and more inhuman forms of dispute... [which] inevitably leads into regions that evoke great 'inhuman energies' which are not ultimately amenable to human control or restraint."[3] In the first level both parties can still win (win–win). In the second level one of the parties loses and the other wins (win–lose), and in the third level both parties lose (lose–lose).



The model describes how two parties in a conflict behave. Solutions leading to de-escalation are not immediately apparent in this model, particularly when it appears to both conflict parties impossible to reverse the situation (e.g. an aggressive act on the territory of a state, separation of a common child from the other parent, withdrawal of nationality by a state, mass redundancy to improve shareholder value), or when one party selects conflict escalation as a strategic ploy.

To achieve de-escalation Glasl assigns the following strategic models to the different stages of escalation:

- Stage 1–3: mediation
- Stage 3–5: process guidance
- Stage 4–6: sociotherapeutic process guidance
- Stage 5–7: intercession, intermediation
- Stage 6–8: arbitration, court action
- Stage 7–9: forcible intervention

The ability to recognise and eliminate conflict-nourishing forces in a culturally neutral and non-judgemental fashion in order to de-escalate a conflict is highly advantageous in particular for managers, consultants and social workers.

[3] Glasl

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Implementation of regulatory framework and control

As noted in the discussion of Task 6, above, the DPO must generally be consulted on any matter relating to data protection that arises within her organisation, including in the drafting of general policy guidelines, etc.

However, there is one matter that is of particular importance in this regard. This is the new explicit requirement of the GDPR (not yet spelled out in the 1995 Data Protection Directive, although it could already be, and was, read into that),434 that controllers embed the principle of "data protection by design and by default" (which includes the principle of "security by design [and default]")435 into all their operations. As it is put in Article 25:

> **Article 25**
>
> **Data protection by design and by default**
>
> 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
>
> 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
>
> 3. …[4]

In the area of implementation of particular data protection measures, synergy potentials between the DPOs and [DPAs] emerge as regards the adoption of sanctions and handling of complaints and queries.

As already mentioned, the DPOs have limited powers of enforcement. The [DPA] will contribute to ensuring compliance with the [GDPR] by taking effective measures in the field of prior [consultations or authorisations] and of complaints and other inquiries.

Measures are effective if well targeted and feasible: the DPO can also be seen as a strategic partner in determining the well targeted application of a measure. The handling of complaints and queries by the DPO at a local level is to be encouraged at least as concerns a first phase of investigation and resolution. The [DPAs may] therefore [be expected to take the view] that DPOs should try to investigate and resolve complaints at a local level before referring to the [DPA]. The DPO should also … consult the [DPA] whenever he/she has doubts on the procedure or content of complaints. This does not however prevent the data subject from addressing him/herself directly to the [DPA] under

[4] The third paragraph stipulates that: "An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article." This is discussed in relation to Task 9, below.

[Article 77(1) GDPR]. The limited powers of enforcement of the DPO also imply that in some cases, the complaint or query must be escalated to the [DPA]. The [DPA] therefore provides for valuable support in the field of enforcement. In turn, the DPO can be relied on to provide information to the [DPA] and to provide follow-up on the measures adopted.[5]

[5] Korff/Georges. p.239

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Organizational audits as well as advice and control visits

Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve.[6]

The effectiveness of these audit (inspection) and sanction powers is underpinned by a further requirement, set out in the second sub-clause of Article 4(4), that providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the competent national authorities to verify compliance with the provisions of paragraph 3. The inventory shall only include the information necessary for this purpose

[6] Article 4 (1)

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

The value added by the data protection organization for a company

Apart from the general protections provided for personal data, the GDPR also defines three types of "health data" that require special protection: data concerning health, genetic data, and biometric data. These are classified as sensitive personal data, and the regulation generally prohibits any kind of processing for these unless explicit consent is given or very specific conditions are met. There are some exceptions; processing is generally permissible for assessing working capacity for employment, for the management of health or social care systems, and services, or for public interest.

As healthcare organizations like private and public hospitals, medical device manufacturers, and health insurance providers manage personal data, including the special categories, their compliance with the GDPR requirements is critical. Healthcare organizations need to invest time and capital in changing their perspective and approach, not just towards GDPR but cybersecurity as well. There are unique challenges that the healthcare industry faces, but there are also effective security solutions that will benefit an organization in the long run.

Healthcare organizations, in particular, benefit from compliance even if they are not based in the EU. The healthcare industry has been a prime target for cybercriminals for years, with attacks ranging from business email compromise (BEC) schemes to data breaches. So complying with the regulation is favorable for healthcare organizations on many levels: They will avoid non-compliance fines, be better protected against hackers, have better protection for valuable customer and enterprise data, and have an advantage over other organizations that don't offer clients the same level of security.

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

If more than 2 answers are given, multiple answers are possible. If there are only 2 answers, only one of them is correct.

Unit 3: Crisis Management

1. Which of the areas mentioned belong to the Internet infrastructure according to ENISA

- ☐ logistics company
- ☐ software programs
- ☐ Network administrators
- ☐ routing protocols

2. What are ENISA's tasks?

- ☐ Provide national authorities and EU institutions with expert advice on network and information security.
- ☐ Act as a forum for sharing best practices.
- ☐ Prosecute violations of data protection.
- ☐ Develop security software.

3. Glasl´s de-escalation takes place in several stages. Please tick which are included

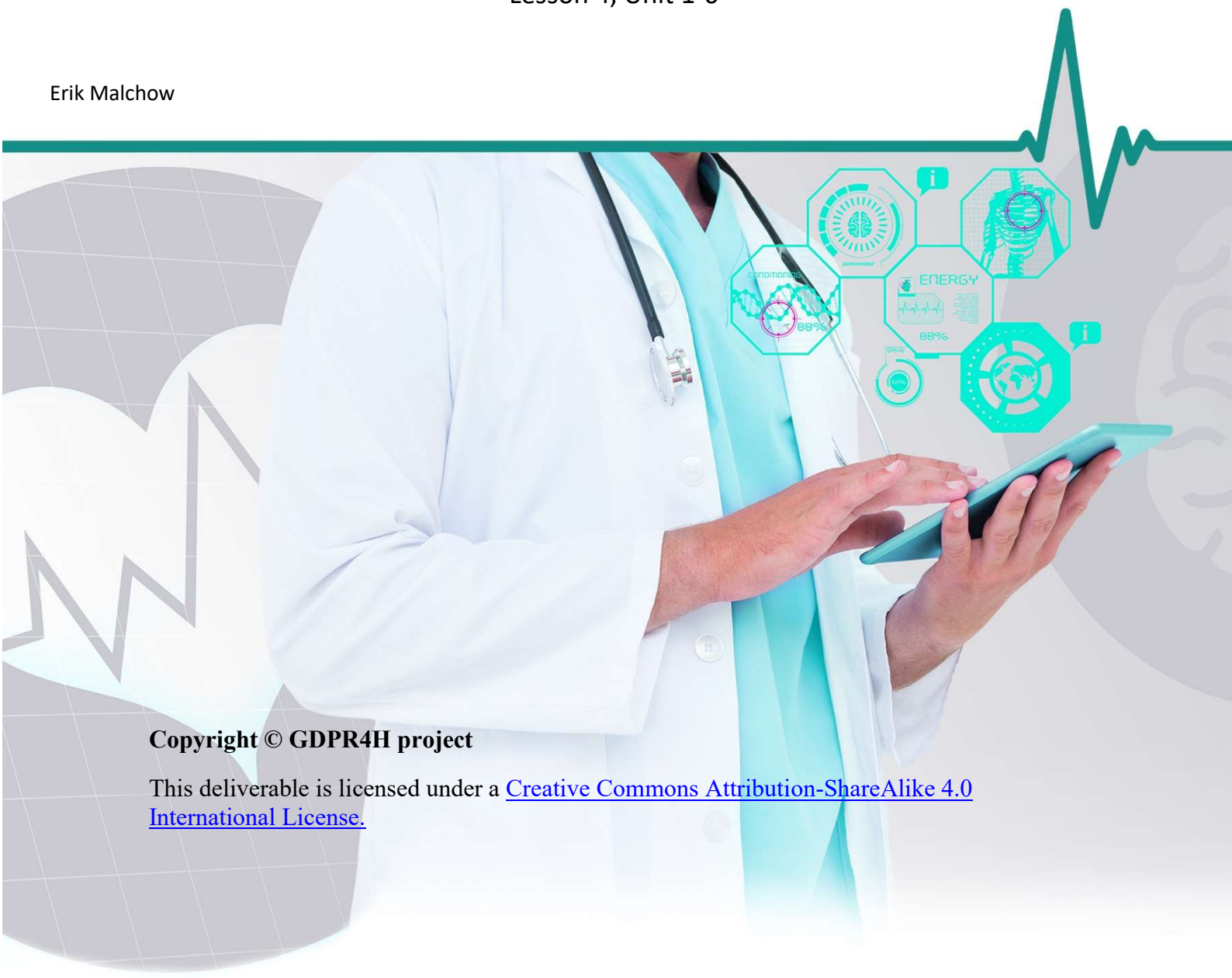
- ☐ Psychotherapy for one of the participants
- ☐ socio-therapeutic process support
- ☐ Force intervention
- ☐ Mediation
- ☐ Formation of coalitions with the most influential people

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Module 3:
Soft Skills for Data Protection Officers

Lesson 4, Unit 1-6

Erik Malchow



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

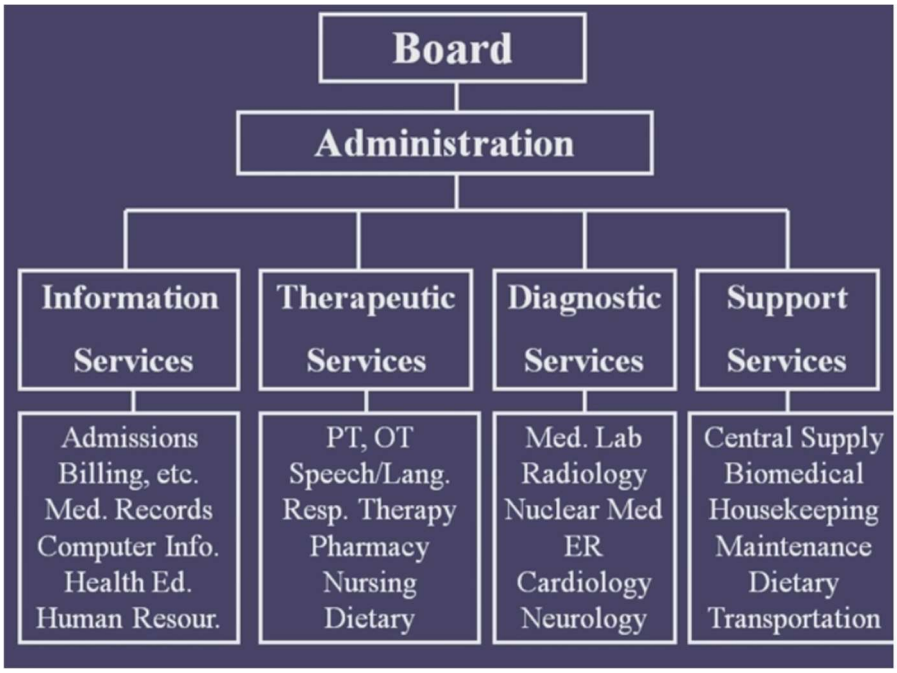
Case Study on data protection implementation

The fourth learning outcome can be seen as a test to trial the achieved competences in communicating data protection policy in healthcare. The DPO will face different situation in an interactive setting that can occur during the setup and maintenance of a data protection policy in a healthcare institution. Previously made up case studies for different situations in the stages of a data protection implementation (e.g. Appointment of a data protection officer, Determining the admissibility criteria, Principles of the DPO according to Article 5 of the GDPR, etc.) will be tested live with the assimilator technique, giving at four possible solutions for a relevant problem. Depending on the group size, this technique can be supported with video footage.

Organogram of a hospital

A DPO can only carry out her tasks in relation to her employer if she is fully cognisant of the internal distribution and allocation of tasks and responsibilities in relation to (or which may involve) any processing of personal data; the external links and arrangements of that organisation with other organisations; and the legal framework(s) for those. Prior to undertaking her main other tasks – except for the carrying out of the initial inventory (register) of personal data processing operations, listed first under the next heading (Task 1), which can be done in parallel – the DPO must therefore map those internal and external links and lines of responsibility in relation to all and every personal data processing operation, and put those in the wider context of her organisation's role and aims, and thoroughly familiarise herself with the relevant rules.

To clarify the internal structures and roles, the DPO must first of all obtain and study the organogram of her organisation, which management should be able to supply her with.



Source: Principles of Health Science, https://www.youtube.com/watch?v=FpQEwbAV3Qw

However, organograms will usually only identify the relevant units and departments in the most general of terms: "human resources", "finance and accounts", "legal", "customer management", etc. (with many public bodies adopting the terminology of private entities, e.g., by referring to welfare claimants as "customers" of the welfare office). They are a useful starting point, but little more than

Steinbeis Hochschule ACQUIN Metropolitan College PEF Skybridge partners crefop arps EMA European Medical Association
Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

that. In in-depth discussions with senior management, including the organisation's legal and ICT officer(s) and, where appropriate, regional or national offices, the DPO should clarify in more detail what exactly the different units and departments are responsible for, including in particular for what purposes each of the units and departments needs, and actually processes, personal data; under what architecture of internal and external technologies this is done; and whether this involves any external technological services or means (including cloud computing). This is where the preliminary scoping overlaps with the carrying out of the inventory of personal data processing operations in Task 1 – but at the preliminary stage, the relevant personal data processing operations need only be identified in broad terms, with reference to the purpose for each such operation, and the technologies used. Moreover, the DPO should at this preliminary phase also already obtain an initial idea of what exact tasks and responsibilities each unit or department has in respect of each personal data operation – i.e., she should identify who is the "business owner" of each operation (to the use the EDPS's terminology).

Examples:

- Population register
- Register of people liable to pay local taxes
- Register of recipients of benefits (e.g., housing benefit or disability benefit)
- Register of clients of social services (e.g., child welfare)
- Registers of imposition of fines (e.g., parking fines)
- Register of permits and licences issued (e.g., to run a bar)
- Register of local police units and officers
- Register of people signed up with local authorities' employment bureaux;
- Register of children in local education
- Register of people issued with official documents (e.g., births, marriages, deaths)
- Register of people buried in local cemeteries
- Register of users of libraries run by the local authorities
- Register of people who have signed up to receive notifications about cultural events
- Accounts
- Human resources

The data protection authority provides the following examples of laws or regulations underpinning the processing of personal data in relation to some of the personal data registers maintained by local authorities, given above.

In addition, it is important that at this stage the DPO (with the help of IT and security staff) also thoroughly familiarises herself with the technical ICT systems, -architecture and - policies of her organisation: the computers (or where they still are used, the manual filing systems) used and whether these include portable and/or mobile devices (and/or personal "own devices" of relevant staff – for which a "Bring Your Own Device [BYOD] policy has to be [put] in place); whether PCs or devices are used online or only offline, on-site or also offsite; what security software and encryption is used, and whether it is fully up-to-date; what the external links and facilities are (including the use of cloud servers, especially if they are based outside the EU/EEA, e.g., in the USA – in which case the relevant data transfer arrangements and contracts need to be checked); whether any of the processing is done by processors (in which case the contracts with them will need to be reviewed);304 what the physical security measures are (doors, rooms, network- and PC passwords,

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

etc.); whether security policies and training is in place; etc., etc. At this preliminary stage those many issues need not all be addressed and resolved – but they should at least be noted, mapped and recorded.

Next, the DPO should try to clarify all the external links that her organisation has to other organisations. Those generally come in two types: (a) the (sister/mother/daughter organisations that the DPO's organisation has formal links with, within what will (in the public sector) usually be an overall hierarchical framework. A local authority may be formally under the immediate jurisdiction of a regional body, which in turn is under the control or supervision of a provincial or federal state body, that at the highest level fits within a wider country-wide public agency, under a national ministry. However, there will be major differences in the arrangements from country to country, or even within a country, including as concerns the relative autonomy that the various bodies have, also in relation to the establishment and management of their personal data processing operations – this is exactly why the DPO should thoroughly familiarize herself with the particular arrangements for her particular organization.

The framework for all the relevant public bodies belonging to a certain hierarchy will be largely defined in formal law, at a range of levels: constitution, statute law, statutory instruments (secondary, binding legislation), ministerial ordnances and instructions, as well as in possible non-binding or non-statutorily-underpinned administrative arrangements, agreements, guidance and policy statements, etc. The processing of personal data by the DPO's organisation may also be covered by a code of conduct, of which there are various types. Again, the DPO should acquire as full and detailed an understanding of those rules and arrangements and codes – and of the processes through which they are adopted, applied and reviewed and amended – as possible, again if needs be with the help of the legal officer(s) of her organisation (and/or by attending courses on the relevant issues if she is not fully cognisant of these issues when taking up her position). There will also be other DPOs in the other organisations belonging to the relevant hierarchy – and it will be crucial for our" DPO to become fully engaged with them, in a DPO network.

Where there is as yet no such network, the DPO should work towards its creation. All the DPOs should of course establish close and good links with the national data protection authority (DPA), including any senior staff members within the DPA with specific responsibilities in relation to public authorities/the kind of public authority to which the DPO's organisation belongs.

Then there are links to external organisations that are outside of the DPO's organisation's hierarchy. Those can include other public authorities in a different hierarchy – for instance, there can be links between educational establishments and welfare institutions, or the police, or between educational authorities in one country and similar organisations in another. Again, there will be (or ought to be) laws covering such links with such bodies, or other formal, binding arrangements and agreements (such as data sharing arrangements and agreements between educational institutions and welfare organisations). The DPO should again obtain full details of all such arrangements whenever these involve or may involve the processing of personal data – and should indeed review them, to see if they adequately reflect, confirm and implement the requirements of the GDPR and of any relevant national data protection laws and -rules – and indeed of more general human rights law.307 The DPO may not be able to challenge a deficient law or legal arrangement as such, but could – and should – notify her employer, and probably the relevant DPA, of her view that the law is deficient.

Steinbeis HOCHSCHULE ACQUIN METROPOLITAN COLLEGE CENTRE OF EXCELLENCE PEF Skybridge partners crefop arps EMA European Medical Association

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Sometimes, the links between, and the cooperation between, formally distinct entities are based on informal, non-public arrangements. However, this is problematic from a data protection point of view.

As part of the preliminary scoping task, the DPO should again check whether any such formal arrangements are in place, and if so, whether they (a) really reflect the practical divisions and attributions of responsibilities and (b) fully meet the requirements of the GDPR. If there is no formal arrangement in place, the DPO should advise that one be drawn up urgently (and she should be involved in the discussion, agreement and recording). If only informal arrangements are in place, the DPO should advise that they be replaced by formal ones.

Moreover, when the links and arrangements with other entities amount to or include controller – controller and/or controller – processor arrangements, those should be underpinned by relevant (GDPR-compliant) controller – controller and/or controller – processor contracts; and when the links and arrangements with other entities involve transfers of personal data to non-EU/EEA countries (so-called "third countries"), the transfers should be based on relevant (GDPR-compliant) data transfer clauses (either standard clauses approved by the relevant DPA or DPAs or by the EDPB, or ad hoc clauses that conform to the GDPR).

Where such contracts or clauses are in existence, the DPO should review them to see if they comply with the GDPR, and where there are no such contracts or clauses, but there should be, the DPO should advise that they be concluded urgently. These tasks of the DPO in relation to formal agreements, controller – to controller- and controller – to processor contracts and data transfer clauses (and in other related respects) are further discussed at 3.x, below. Here, it will suffice to note that the DPO should identify such issues in the preliminary scoping task, to then be addressed thereafter.

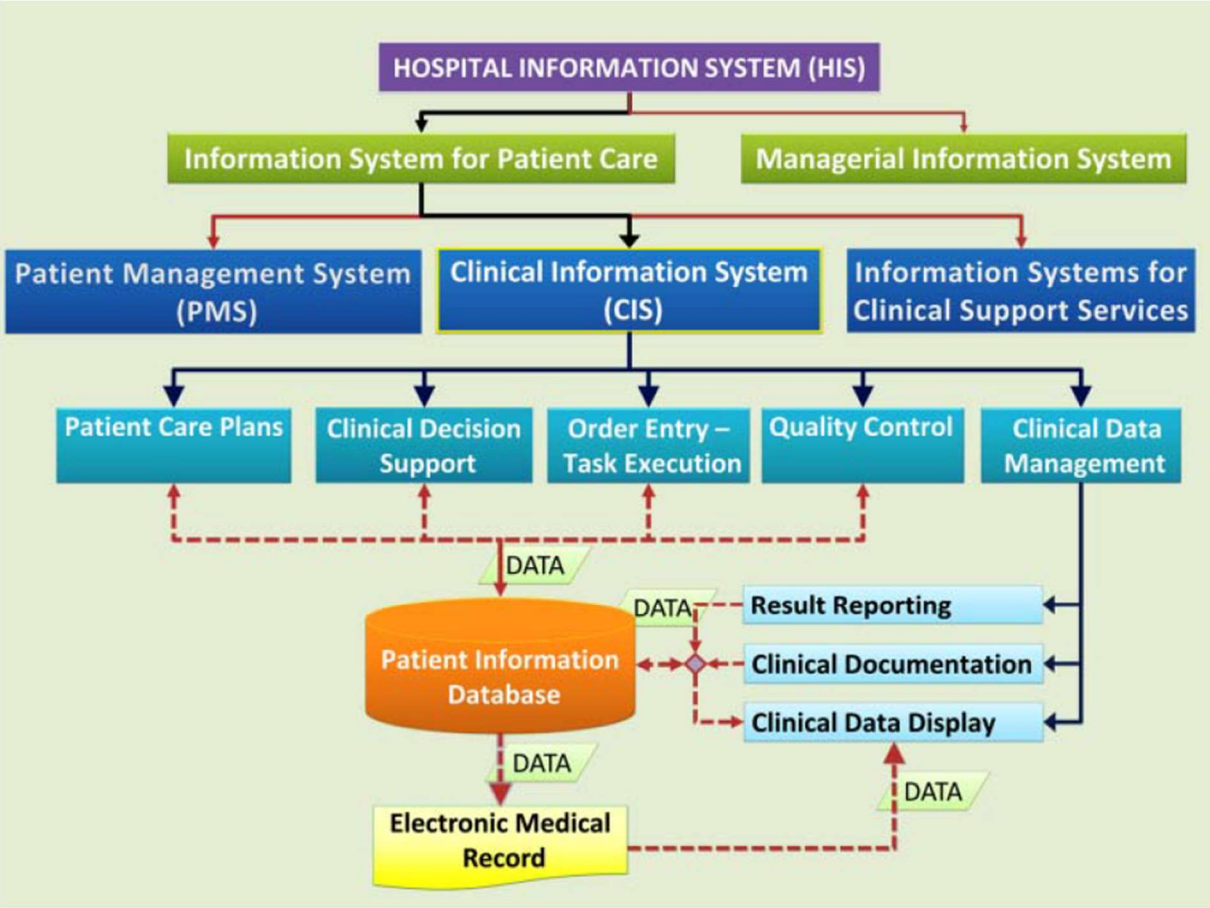
Finally, the DPO's organisation will have links with external (private- and public-sector) suppliers of goods or services, ranging from outsourced data processing, accounting and website management to the supply of canteen meals, maintenance and repairs, staff medical and wellbeing support, etc., etc. The work done in these respects will be based on contracts (either ordinary civil contracts or special public-private contracts). Those contracts will also be the basis for – and ought to specifically address – any processing of personal data by the parties to those contracts: for the collecting of the relevant personal data to the sharing and use of those data, to their final destruction or erasure. If the other entity is a controller in its own right, those contracts (or at least the data protection-relevant elements of those contracts) will, in data protection terms, constitute controller-to-controller personal data processing contracts. If the other entity acts merely as a processor for the DPO's organisation, the contract will be a controller-processor contract. And if under the contract personal data are transferred to a place outside the EU/EEA (typically, to a "cloud" server maintained by the contractor), those contracts constitute personal data transfer contracts.

In the preliminary scoping exercise, the DPO should again identify whether there are such contracts, and then, shortly after the scoping exercise, review them, and where they are missing or deficient in GDPR terms, advise that they should be drawn up or revised.

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Mapping the organisation's processing activities in broad terms

Once the DPO has carried out the general scoping of her organisation (as set out above), he or she will be able to map the organisation's personal data processing activities in broad terms, as a crucial step towards the creation of a detailed register of all those activities and all the individual personal data processing operations, carried out in Task 1 (discussed next). This should lead to a chart such as the one provided here, setting out the "Functional Components of a Clinical Information System".



Source: Dr Abdollah Salleh, https://drdollah.com/hospital-information-system-his/

Note that the above map is more closely related to personal data processing operations than the organogram of a hospital, provided earlier.

Creating a register of personal data processing operations

Subject to a limited exemption discussed below under that heading, under Article 30 GDPR, each controller must "maintain a **record** of processing activities under its responsibility", listing various details of each operation such as the name of the controller (and, one may add, of the "business owner") of the operation, the purpose(s) of the operation, the categories of data subjects, personal data and recipients, etc. This duty to keep a register of processing operations is closely linked to the accountability principle, discussed at 2.2, above, by facilitating effective supervision by the relevant data protection authority ("supervisory authority") – as is underlined by Recital (82) of the GDPR:

In order to demonstrate compliance with this Regulation, the controller or processor **should maintain records of processing activities** under its responsibility.

Although, as with most other requirements of the GDPR, this is formally a duty of the controller rather than the DPO, in practice it will be the DPO who will either be in charge of this work (in close cooperation with the controller's relevant staff), or who will at the very least be closely involved in it and oversee it.
In practice, DPOs often create inventories and hold a register of processing operations based on information provided to them by the various departments in their organisation responsible for the processing of personal data. This practice has been established under many current national laws and under the data protection rules applicable to the EU institutions and bodies.

For a new DPO, this requires first of all the (overseeing of the) carrying out of an inventory of all the processing operations of the organisation that may involve the processing of personal data and of links with other organisations. This involves considering what data do constitute such data – which is not always straight-forward.

An initial, basic inventory can usefully be carried out in parallel with the broader scoping of the organisation and its operational context, in the preliminary task (Task 0), described above. Subject to the exemption, noted below, this should then be followed by a full inventory.

The full inventory should lead to the creation of the register (the collection of "records") of all of the controller's personal data processing operations, mentioned in Article 30 (as discussed a little later in this section, under the heading "Contents and structure of the register entries") – which should thereafter be kept up-to-date by the DPO (or the DPO should at least ensure that it is kept up to date): see the text below, under the heading "(ongoing) Monitoring of compliance".

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Reviewing the personal data processing operations

For the DPO, after having created the register of her organisation's personal data processing operation (Task 1), the next step is the carrying out of an in-depth review of all the registered personal data processing operations, to see whether they meet the requirements of the GDPR in all relevant respects, including in respect of:

- purpose-specification and -limitation;
- the validity of any consent (and the existence of documentary proof of consent having been given) or the applicability of any other legal basis for the processing;
- personal data processed and their relevance and necessity in relation to the specified purpose(s));
- data quality (accuracy, up-to-dateness, etc., of the data, as well as data minimisation and pseudonymisation);
- information provided to the data subject of the controller's own motion (either when data are collected from the data subject or otherwise, or on request – also in relation to data collected from website visitors);
- the length of time for which the data are retained in identifiable form and any information as to de-identification;
- technical, organisational and physical data security (including physical access limitation and technical access limitation [user name, passwords, PINs policies, etc.], encryption, etc.);
- cross-border data transfers (and the legal and other contractual or other arrangements for them);
- etcetera.

In the light of the findings on the above, the DPO should be able to assess:

- whether the processing operation as a whole can be said to comply with the overriding principle of lawfulness and fairness.

The DPO asking and answering the following relevant questions:

- Is it sufficiently clear which entity is the controller of the personal data processing operation, and if any other entities are involved, what their respective status is (e.g., joint controller, processor, or separate third party controller)? If this is not obvious, are formal arrangements in place that clarify these issues?

- Is it sufficiently clear which business unit is the "business owner" in respect of the personal data processing operation (i.e., which has day-to-day de facto responsibility for the processing)? Is this set out in a formal document (e.g., specific instructions from the controller to the unit)?

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

- Is the purpose, or are the purposes, of the personal data processing operation specified in sufficiently precise terms? Where (i.e., in what kind of document)? If the personal data used in the processing operation are used for more than one purpose, what is the primary purpose and what is or are the secondary purpose(s)? Are those secondary purposes compatible with the primary purpose, or are they separate purposes?

- Are the personal data that are processed adequate, relevant and necessary for the primary purpose? How is it ensured that they are and remain accurate and up to date for this purpose, and what arrangements are made to ensure this and to rectify or up-date or erase inaccurate or out of date information? Are the measures taken adequate and sufficient? Would it be possible to achieve the

same purpose with less risk to the privacy and other rights of the individuals concerned?

- What personal data are used or disclosed for any secondary purposes or indeed new, unrelated purposes (typically, to a third party)? Are the personal data that are processed adequate, relevant and necessary for those secondary or new, unrelated purposes? (If all the data collected for one [primary] purpose are disclosed unthinkingly for a/any secondary purpose or purposes or a new, unrelated purpose, they, or some of them, may well be excessive for that secondary or unrelated purpose or those secondary or unrelated purposes. Has this been considered?)

- How is it ensured that the data that are used or disclosed for secondary or new, unrelated purposes are accurate and up to date for those secondary or new purposes at the time of first use or disclosure for those purposes, and what arrangements are made to ensure they remain accurate and up to date after that first use or disclosure, and are rectified or up-dated or erased as and when they become inaccurate or out of date? Are the relevant measures adequate and sufficient?

- When, how, from whom and in what form are which of the personal data obtained? E.g.: the data subject, a government department, a (former) employer, etc.; e.g., on paper, by electronic transfer, etc.

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Assessing the risks posed by the personal data processing operations

As noted above, the GDPR imposes a general duty on controllers to "[take] into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons" posed by each personal data processing operation, and to "implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation" (Art. 24(1); cf. also Art. 25(1))).

The DPO, too shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Compliance with these requirements demand that the relevant risks be ascertained. This should be done in connection with the carrying out of the inventory of personal data processing operations and the creation of the register of those operations (Task 1) and, especially, with the review of those operations (Task 2).

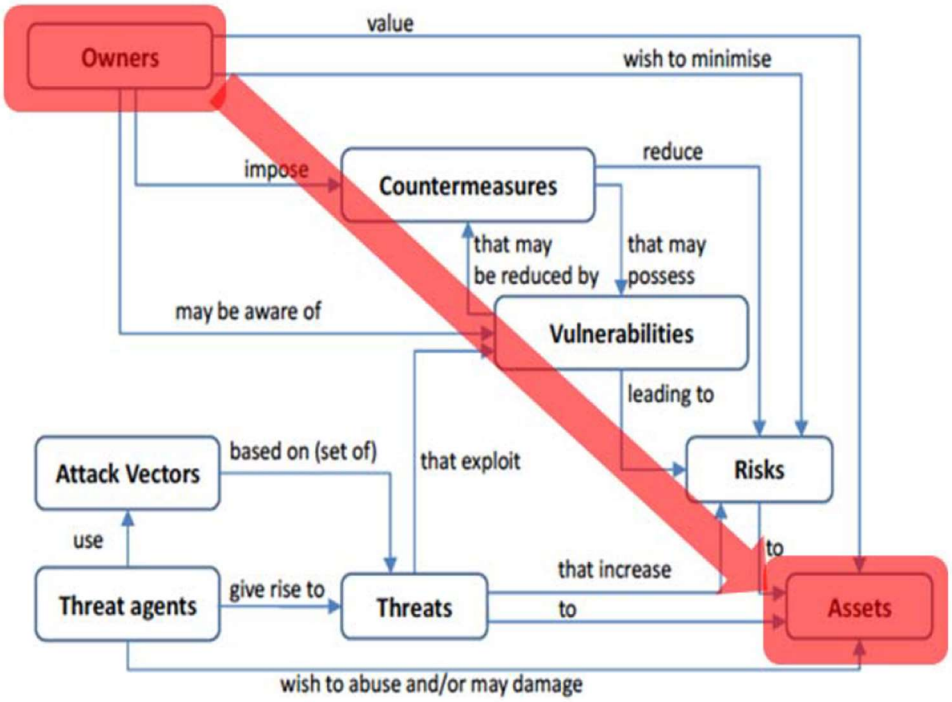
The GDPR does not expressly require the involvement of the DPO in any general risk assessments: it stipulates such involvement only in relation to the more in-depth Data Protection Impact Assessments (Art. 35(2) – see Task 4, below). However, in practice it would be highly advisable (to say the least) to involve the DPO also in these more general risk assessments. Indeed, in practice, the assessment will often depend on the views of the DPO.

It should be noted that the risks to be assessed are not just the security risks in a narrow sense – i.e., the likelihood and impact of a data breach335 – but rather, the risks to the rights and freedoms of the data subjects (and other individuals) that may be posed by the processing operation. This includes not only their general rights to privacy and private life as well as their specific data subject rights, but also, depending on the case, their rights to freedom of expression, freedom of movement, freedom from non-discrimination, freedom from authoritarian power and the right to stay in a democratic society without undue surveillance by their own, or by other countries, and the right to an effective remedy.

All this underlines that for the general review and the risk assessment, the controller – in practice, the DPO – must look closely at all aspects of each distinct personal data processing operation and -function.

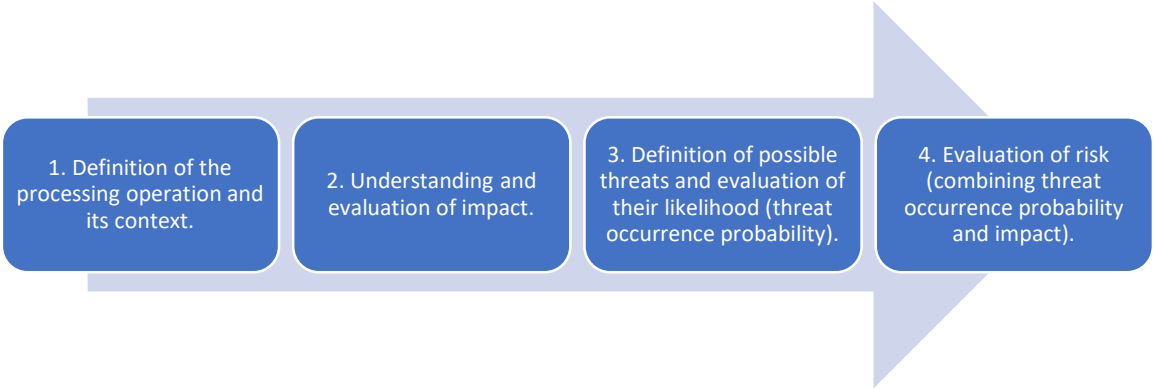
Steinbeis HOCHSCHULE ACQUIN METROPOLITAN COLLEGE CENTRE OF EXCELLENCE PEF Skybridge partners crefop arps EMA European Medical Association
Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

As proposed by the Italian data protection authority, it is useful to follow the approach adopted by ENISA (the EU Agency for Network and Information Security), which in turn builds on the widely accepted standard ISO 27005: "Threats abuse vulnerabilities of assets to generate harm for the organisation"; and to consider in more detailed terms risk as being composed of the following elements: Asset (Vulnerabilities, Controls), Threat (Threat Agent Profile, Likelihood) and Impact. The elements of risk and their relationships can then be illustrated as follows:



Source: ENISA Threat Landscape Report 2016: The elements of risk and their relationships[1]

A proper risk assessment involves four steps:



[1] according to ISO 15408:2005, https://www.enisa.europa.eu/publications/enisa-threat-landscapereport- 2016. See also its 2017 report, https://www.enisa.europa.eu/publications/enisa-threatlandscape- report-2017.

Steinbeis HOCHSCHULE ACQUIN METROPOLITAN COLLEGE CENTRE OF EXCELLENCE PEF Skybridge partners crefop arps EMA European Medical Association
Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

The person assessing the security risk can, from these answers, then calculate the threat occurrence probability, as indicated in the charts. This score can then be combined with the impact score to arrive at an overall risk score, as indicated in the chart after those.

1.1.1. Threat occurrence probability

In order to fill the table below for the calculation of a threat occurrence probability , use the questions on the next page for the mentioned four categories.

Assessment area:	Nr of "yes" answers	Level	Score
A. Network & technical resources:	0 - 1	Low	**1**
	2 – 3	Medium	**2**
	4 – 5	High	**3**
B. Processes & procedures	0 - 1	Low	**1**
	2 – 3	Medium	**2**
	4 – 5	High	**3**
C. Parties & people involved	0 - 1	Low	**1**
	2 – 3	Medium	**2**
	4 – 5	High	**3**
D. Business sector & scale	0 - 1	Low	**1**
	2 – 3	Medium	**2**
	4 – 5	High	**3**

Steinbeis HOCHSCHULE ACQUIN METROPOLITAN COLLEGE CENTRE OF EXCELLENCE PEF Skybridge partners crefop arps EMA European Medical Association

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

THE FOUR MAIN ASSESSMENT AREAS IN TERMS OF DATA SECURITY:

A. Network & technical resources:	B. Processes & procedures	C. Parties & people involved	D. Business sector & scale
1. Is any part of the processing of personal data performed through the internet?	6. Are the roles and responsibilities with regard to personal data processing vague or not clearly defined?	11. Is the processing of personal data performed by a non-defined number of employees?	16. Do you consider your business sector as being prone to cyberattacks?
2. Is it possible to provide access to an internal personal data processing system through the internet (e.g. for certain users or groups of users)?	7. Is the acceptable use of the network, system and physical resources within the organization ambiguous or not clearly defined	12. Is any part of the data processing operation performed by a contractor/third party (data processor)?	17. Has your organization suffered any cyberattack or other type of security breach over the last two years?
3. Is the personal data processing system interconnected to another external or internal (to your organization) IT system or service?	8. Are the employees allowed to bring and use their own devices to connect to the personal data processing system?	13. Are the obligations of the parties/persons involved in personal data processing ambiguous or not clearly stated?	18. Have you received any notifications and/or complaints with regard to the security of the IT system (used for the processing of personal data) over the last year?
4. Can unauthorized individuals easily access the data processing environment?	9. Are employees allowed to transfer, store or otherwise process personal data outside the premises of the organization?	14. Is personnel involved in the processing of personal data unfamiliar with information security matters?	19. Does a processing operation concern a large volume of individuals and/or personal data?
5. Is the personal data processing system designed, implemented or maintained without following relevant best practices?	10. Can personal data processing activities be carried out without log files being created?	15. Do persons/ parties involved in the data processing operation neglect to securely store and/or destroy personal data?	20. Are there any security best practices specific to your business sector that have not been adequately followed?

Source: Korff/Georges, p. 182

Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, health-, genetic- or biometric data, and data on sexual orientation), as well as personal data relating to criminal convictions or offences as defined in Article 10.

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Beyond these provisions of the GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals. These personal data are considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (see the third example, below), or because they impact the exercise of a fundamental right (see the fourth example) or because their violation clearly involves serious impacts in the data subject's daily life (see the fifth example). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment, [taking into account whether the data subject could reasonably expect that the data might be used by other people for certain purposes: see the seventh example, below]. For example: A general hospital [or a welfare office] keeping patients' [or welfare claimants'] medical records.

As detailed above, the GDPR requires that, in the case of a breach, the controller shall notify the breach without undue delay and, where feasible, not later than 72 hours after having become aware of it. This may raise the question of when a controller can be considered to have become "aware" of a breach. WP29 considers that a controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.

However, as indicated earlier, the GDPR requires the controller to implement all appropriate technical protection and organisational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject21. This puts an obligation on the controller to ensure that they will be "aware" of any breaches in a timely manner so that they can take appropriate action.

When, exactly, a controller can be considered to be "aware" of a particular breach will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Examples

1. In the case of a loss of a USB key with unencrypted personal data it is often not possible to ascertain whether unauthorised persons gained access to that data. Nevertheless, even though the controller may not be able to establish if a confidentiality breach has taken place, such a case has to be notified as there is a reasonable degree of certainty that an availability breach has occurred; the controller would become "aware" when it realised the USB key had been lost.
2. A third party informs a controller that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure. As the controller has been presented with clear evidence of a confidentiality breach then there can be no doubt that it has become "aware".
3. A controller detects that there has been a possible intrusion into its network. The controller checks its systems to establish whether personal data held on that system has been compromised and confirms this is the case. Once again, as the controller now has clear evidence of a breach there can be no doubt that it has become "aware".
4. A cybercriminal contacts the controller after having hacked its system in order to ask for a ransom. In that case, after checking its system to confirm it has been attacked the controller has clear evidence that a breach has occurred and there is no doubt that it has become aware.
5. An individual informs the controller that they have received an email impersonating the controller which contains personal data relating to his (actual) use of the controller's service, suggesting that the security of the controller has been compromised. The controller conducts a short period of investigation and identifies an intrusion into their network and evidence of unauthorised access to personal data. The controller would now be considered as "aware" and notification to the supervisory authority is required unless this is unlikely to present a risk to the rights and freedoms of individuals. The controller will need to take appropriate remedial action to address the breach.

A breach that would not require notification to the supervisory authority would be the loss of a securely encrypted mobile device, utilised by the controller and its staff. Provided the encryption key remains within the secure possession of the controller and this is not the sole copy of the personal data then the personal data would be inaccessible to an attacker. This means the breach is unlikely to result in a risk to the rights and freedoms of the data subjects in question. If it later becomes evident that the encryption key was compromised or that the encryption software or algorithm is vulnerable, then the risk to the rights and freedoms of natural persons will change and thus notification may now be required.

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.