Lower Saxony Audit Questionnaire 2018/19

LOOSELY TRANSLATED

Question 1: Preparation for the GDPR

How did you prepare as a company for GDPR and the DPA 2018? Describe (briefly) the procedure you followed, which areas were involved, and which measures were initiated. If you have not completed the process, please also explain the implementation status.

Note: The purpose of this question was to obtain an overview of the different approaches of companies as well as their self-assessment regarding their position on the road to implementation of the GDPR. An evaluation of the methodology does not explicitly take place.

1. Have we identified all the main business sectors involved in processing personal data (e.g. human resources, IT, sales / customer service, marketing)?
2. Is there evidence that GDPR training has been carried out?
3. Have all the measures planned by the organisation been implemented?

+

Question 2: List of processing activities (VVT)

How did you ensure that all your business processes involving the processing of personal data were included in the Article 30 records of processing activities? How do you keep it up to date? Please provide an overview of your documented procedures and an example of how you put the records together.

Art. 30 GDPR

1) Have existing procedures have been adapted to GDPR or new procedures have been produced?

2) Are the records of processing activities regularly reviewed and updated as necessary?

3) Is it clear from a review of policies and procedures that standard procedures for e.g. office communication, personnel administration, payroll, application management, homepage and customer administration are documented?

4) Do the organisation's procedures comply with the requirements of Art. 30?

- Are the name and contact details of the DPO set out?
- Are - where applicable - the name and contact details of joint controllers set out?
- Are - where relevant - name and contact details of the representative set out?
- Are - where relevant - the name and contact details of any existing data protection specified orders?
- Are the purposes of processing set out?
- Are the categories of affected data subjects (eg employees, customers, etc.) and the categories personal data (e.g. employee master data, applicant data, customer contact details, credit data, etc.) clearly described?
- Are the categories of recipients of personal data clearly set out?
- Is there a clear statement concerning the transfer of personal data to a third country or to an internal organisation?
- Are the deadlines for the deletion of the various categories of personal data set out?
- Is a there at least a general description of the technical and organisational security measures?

+

Question 3: Admissibility of processing

Based on which legal bases do you process personal data? Unless you are based too of personal information, please attach your patterns.
Art. 6, 7 and 8 DS-GVO
1. Are the above legal bases plausible on the basis of the submitted procedure overview?
2. Are the declarations of consent easy to understand, ie content of the person concerned the "whether" and "how" of giving consent in a clear and simple language guided?
3. Is the identity of the person responsible indicated?
4. Is the purpose of the processing mentioned?
5. Is the type of data collected and used known?
6. Is the right of withdrawal noted?
7. Is it apparent from the documents that the revocation is as simple as the granting of consent? supply?
8. Are there indications that the characteristic of voluntariness could be missing?
9. Does it become clear from the documents that the consent is documented?

+

Question 4: Data Subject+ rights

How do you ensure compliance with the data subject rights (for information, information, correction, deletion, limitation of processing, data portability)? Show how your GDPR project paying particular attention to how you comply with your information rights obligations.

1. Information according to Art. 13 and 14 (sample):

- Has the organisation produced clear transparency information?
    - Is this information readily available (e.g. notices, flyers, e-mails)?
    - Is the information clearly displayed (eg by headings, paragraphs, insurance)?
    - Is the information understandable and formulated in simple language? The text should be unambiguous, avoiding jargon, or technical terms.
    - Are the Data Protection Officer's details clearly available?
    - Are the purposes of the processing and the legal basis clearly set out?
    - If replying on legitimate interest, has the legitimate interest clearly been described?
    - Are the recipients or categories of recipients of personal data clearly described?
    - Are international transfers of personal data clearly set out?
    - If personal data is transferred to a country without an adequacy decision, is the safeguard for transfer clearly identified?
    - Are subjects informed how long their data will be retained for?
    - Are subjects informed about all of their data protection rights, including the right to withdraw consent and the right to complain to the ICO?
    - Is reference made to the legal or contractual obligation to process?
    - Is passed through an automated decision-making process (eg profiling) logic and the implications and intended effects of such Processing for the affected person informed?
    - If an intended change of purpose ensures that the data subject is present This processing information about this other purpose and all others relevant information (see above, points 1 to 4)?
    - Is there a privacy policy on the site?

    - Is the privacy policy easy to find (max 2 clicks from the start page)?
    - Is the privacy policy understandable and in plain language?

2. Right to information
- Is there are a clear procedure for dealing with subject access requests that logical and properly worked out? Is it available to all staff?
- Does it clearly set out how the identity applicants is properly checked?
- Does the procedure make clear that information should be provided promptly and in all cases within one month of receipt?
- Is it clear who will find and provide the data?

Note: applicants should receive the following:
- *purposes*
- *categories of personal data processed*
- *all recipients or categories of recipients to whom the personal data has been disclosed or yet to be disclosed*
- *all recipients in third countries or int. Organizations*
- *the planned storage period or, if this information is not possible, the criteria for determining the storage duration*
- *the existence of a right of appeal to a supervisory authority*

+

3. Right of rectification
- Is the procedure for the right to rectification clearly and specifically documented?
- Does it clearly set out how the identity of applicants is properly checked?
- Does the procedure make clear that information should be rectified promptly and in all cases within one month of receipt where the request is valid?
- Does the procedure set out how recipients of inaccurate data will be notified of any correction?

4. Deletion
- Is the procedure for the right to erasure clearly and specifically documented?
- Does it clearly set out how the identity of applicants is properly checked?
- Does the procedure make clear that information should be erased promptly and in all cases within one month of receipt where the request is valid?
- Does the procedure set out under what conditions data should be deleted?

5. Restriction of processing
- Is the procedure for the right for restriction clearly and specifically documented?
- Does it clearly set out how the identity of applicants is properly checked?
- Does the procedure make clear that information should be restricted promptly and in all cases within one month of receipt where the request is valid?
- Does the procedure describe how the applicant will be informed that data has been restricted and when the restriction is lifted?
- Does the procedure set out how recipients of data that has been restricted will be informed of successful restrictions?

6. Data portability
- Is the procedure for the right to apply for a portable copy of some data clearly and specifically documented?

- Does it clearly set out how the identity of applicants is properly checked?
- Does the procedure make clear that portable data should be provided promptly and in all cases within one month of receipt where the request is valid?
- Is it clear how data is provided in a common, structured and machine-readable format this is easy to identify, extract and open)?

+

Question 5: Security measures

a. How do you ensure that your technical and organisational measures or those of your service providers ensure a level of protection appropriate to the processing risk?

- Has the organisation set out a risk-based approach to information security?
- Can the organisation demonstrate that the level of security is appropriate to the identified risks?
- Has the organisation taken into account the cost and current state of the art of available security measures?
- is the organisation clearly aware that even if data is being processed by a service provider, they retain legal responsibility?

b. How do you make sure that your technical and organizational measures are appropriate?

- Has the organisation properly understood "state of the art" (i.e. the best currently available technology?)
- Can the organisation demonstrate that its security measures have taken into account what
- state of the art currently is?
- Does the organisation continuously monitor the current state of developments in security?
- Does the organisation review its security measures to ensure that they reflect the most up-to-date measures?

c. How do you make ensure that you are applying security in the most appropriate way?

- Do your security measures take into account the different roles and responsibilities of those using personal data?

d. How do you ensure that when changing or redeveloping products or services, privacy requirements from the start (Data Protection by Design and by Default)?

- Can the organisation demonstrate the proper data protection compliance is the default setting?
- Can the organisation demonstrate throughout the data lifecycle that data protection issues are observed and complied with?
- Does the organisation consistently minimise the amount of data used?
- Is the processing of data transparent?

+

Question 6: Privacy Impact Assessment

a. How do you ensure that Data Protection Impact Assessments are carried out?

1. How do you ensure that you carry put impact assessments that are required by Article 35 of the GDPR?

2. What methodology for risk assessment is used? (e.g. guidance from the EDPB or the ICO)

- If using your own method, how have you ensured that it is suitable for identifying high-risk processing?
- Does your methodology set out who is responsible for carrying out the DPIA?
- Does it set out how you document which processing meets the threshold for a DPIA and which does not?

PICK AN EXAMPLE OF HIGH RISK PROCESING

- Identify an example of high-risk processing – how have the risks been dealt with?
- Does the example include a systematic description of the processing and the purposes?

For the example of high-risk processing, was a DPIA carried out?

- Yes
- No, because no high risk
- No, because a DSFA has already been done for a similar process
- No, because the processing started before 25 May 2018 and the risks have not changed since then

Did you assess necessity and proportionality of the processing?

- Is the need for processing clearly identified?
- Is that need justified?
- Is the proportionality of the processing identified?
- Is the proportionality of the processing justified?

Is there an assessment of the risks to the rights and freedoms of data subjects?

- Is the risk assessment method documented?
- Have the following objectives are considered: confidentiality and integrity of data, availability, transparency, involvement of a human being in automated decisions?
- Have the risks been identified ?
- Has the severity of the damage been assessed?
- Is the assessment of the seriousness of the damage justified?
- Is the likelihood of the risk set out?
- Is the assessment of likelihood justified?
- If the reasons are given taking into account the nature, extent, circumstances and
- the processing?
- Are sources of risk named? e.g. hackers, hardware failure, own employees

Remedial measures

- Are remedies for risks clearly identified?
- Do the remedies address the identified risks?
- Do the remedies account for the implementation costs?
- Do the remedies reflect the state of the art of technology and other issues?
- Is there any residual risk?
- If there are residual risks, have you examined whether to carry out prior consultation?
- Has the Data Protection Officer been consulted? If not, why not?
- Have relevant data subjects been consulted? If not, why not?

+

Question 7: Contracts

Have you adapted your current contracts to comply with GDPR?
If you use model contracts, please attach them, and in addition please add a current sample contract with one of your processors.

1. Overall, do existing contracts comply with the requirements of the GDPR?

2. Do the model contract (if used) and the submitted sample contract meet the requirements of Article 28?

- Is the purpose of processing specified in the contract?
- Is the duration of the agreement fixed?
- Does the contract contain information on type (e.g. collection, organisation, adaptation, dissemination or destruction of data) and purpose of processing?
- Are the types of personal data and the categories of data subjects specified?
- Is the person responsible for the processing clearly identified?
- Does the contract cover arrangements regarding the transfer of personal data to a third party or an international organization?
- Does the contract ensure that data is only processed by authorised persons (i.e. to comply with GDPR's requirements on confidentiality)
- Does the contract require the processor to have relevant technical and organisational measures in place?
- Does the contract stipulate that the controller must consent to the use of and changes to subcontractors?
- In the case of approved subcontracting, does the contract require that the subcontractor imposes the same obligations as the processor?
- Does the contract require the processor to support the controller when data subjects exercise their rights?
- Does the contract require the processor to have measures to comply with their own obligations set out in GDPR Articles 32 to 36 (security, impact assessments etc)?
- Is the processor explicitly required to delete or return of all personal data at the end of the contract?

+

Question 8: Data Protection Officer

How is your Data Protection Officer involved in your organisation? What qualifications do they have?

1) Location and responsibilities of the DPO:

- Does the DPO report directly to the highest level of senior management?
- Does the DPO have other responsibilities within the organisation?
- If so, what position do they hold in the company?
- Does the other role represent a risk of bias and thus a conflict of interest? (e.g. DPO is owner, board, management or HR or IT)

2) External DPO:

- Is there a risk of bias and thus a conflict of interest? (e.g., because the external DPO is also a service provider for IT Services)

3) DPO's knowledge

- Can the DPO's current, specific knowledge of the legislation be discerned from documents provided? For example, what education and training in data protection have they

undergone, what is the extent of their experience (duration) in data protection, what relevant qualifications do they have training (e.g. lawyer, records management), do they participate in established data protection networks?

4) Publication of the DPO's contact details

- Are the DPO's contact details published on the company's website?
- Is the contact information easy to find there? (max 2 clicks from the start page)

5) Has the DPO registered with the ICO?

+

Question 9: Reporting obligations

Are personal data breaches properly reported?

- Is the process of reporting personal data breaches clearly identifiable?
- Are the responsibilities (i.e. who does what) clearly set out in the notification process?
- Is the 72-hour deadline clearly set out?
- Is it clear which staff have been made aware of the process?
- Does the process show that data protection breaches are clearly documented?

+

Question 10: Documentation

How can you demonstrate your compliance with all of the above obligations?