# Standard questionnaire guide

|  |  |
| --- | --- |
| Helping you establish an overview | The General Data Protection Regulation (GDPR) will come into force on 25 May 2018. Prior to this date, it is DI’s recommendation that our member companies establish an overview of the measures and changes you have to implement in order to comply with the many new requirements of the Regulation. |
| The questionnaire | Establishing a detailed overview of all the company’s processing of personal data can be a great help when it comes to identifying the areas in which there is a need to increase the current compliance level. DI has in collaboration with Bruun & Hjejle prepared a general standard questionnaire that may be used for this purpose.  It is up to you to decide whether to conduct a dataflow analysis. It may help you establish an overview for your preparation of the compulsory documentation, and at the same time it can provide insight into areas, if any, that demand an effort for you to comply with the rules. |
| Before you complete the questionnaire | Before you complete the questionnaire, you must establish an overview of the processes in the company that involve processing of personal data. A process is made up of a series of correlated processes and activities, e.g. hiring employees, direct marketing, travel expense settlements and controls etc. You can read more about process identification and dataflow identification in our process mapping guide [LINK]. |
| After you have completed the questionnaire | When the questionnaire is completed, you can prioritise – either by yourselves or by external support – the areas in which measures are needed in order to comply with the rules of the GDPR. |

The questionnaire consists of five sections.

Section 1 is to be completed for all processes that involve processing of personal data. In this section, you must disclose whether you are the data controller or the data processor in relation to the processing activity.

If you are the **data controller**, you must complete sections 1-3. If there are several types of data subjects in the same process, you must complete section 2 for each type of data subject.

If you are the **data processor**, you must complete sections 1 and 4.

Section 5 concerns general compliance and will therefore be advantageous to complete for the company as a whole.

# Section 1 – Overview of the process

|  |  |  |
| --- | --- | --- |
| Question |  | |
| Company name | [The name of the company] | |
| Department of the company involved in the process | [Departments] | |
| Questionnaire completion date | [Date] | |
| Contact details of the person completing the questionnaire (e.g. the project lead) | Name: [Name]  Position: [Position]  Email: [Email] | Direct phone: [Phone number]  Cell: [Cell number] |
| Description of the process | [Brief, general description of the process – the general purpose, categories of persons and underlying purposes] | |
| What is your company’s role in the data processing?  A **data controller** is the person or entity who, alone or with others, dertermines for which purposes and how personal data are processed – you may for example be data controller for your employees’ personal data, but you may also be data processor for another group unit, if you manage hosting of their personal data. A **data processor** may also process personal data on behalf of e.g. a client. | [ ] Data controller  [ ] Data processor | |

# Section 2 – Personal data and processing

|  |  |  |
| --- | --- | --- |
| **Subject** | **Question** | **[Insert category of data subjects, e.g. client, employee or the like]** |
| **Ordinary personal data**  **(for special categories of personal data and national registration numbers, see below)** | 1. Please describe which ordinary personal data you process in this process. Please state whether the process includes children and adolescents under the age of 16.   E.g.: Name, private and work contact information (email, phone number, home address), sex, date of birth, photograph and employee ID-number. |  |
| 1. What is the purpose of the processing of the ordinary personal data?   E.g. marketing, recruitment, etc. |  |
| **Special categories of personal data** | 1. Please tick the special categories of personal data that you process in this process, if any. | [ ] a. racial or ethnic origin  [ ] b. political opinions  [ ] c. religious or philosophical beliefs  [ ] d. trade union membership  [ ] e. genetic data or biometric data for the purpose of uniquely identifying a natural person  [ ] f. data concerning health  [ ] g. data concerning sex life or sexual orientation  [ ] h. criminal convictions and offences or related security measures |
| 1. What is the purpose of processing the special categories of personal data? |  |
| **National identification numbers** | 1. Do you process national identification numbers in this process? | [ ] Yes  [ ] No |
| 1. What is the purpose of processing national identification numbers? |  |
| **Accuracy and updating** | 1. Do you ensure that the personal data are accurate and updated and not comprising more than necessary to fulfil the purposes? | [ ] Yes   * Please describe how [insert description]   [ ] No |
| **Deletion** | 1. Have time limits for deletion of personal data been set? | [ ] Yes   * Please state the time limits for deletion, the basis for the time limit, and whether they are complied with: [insert description]   [ ] No |

|  |  |  |
| --- | --- | --- |
| **The basis for the processing of the personal data** | 1. What is the basis for collecting and processing of the general personal data? | [ ] Consent [Please specify how consent is given and what it covers]  [ ] Contract performance (contract to which the data subject is a party) [Please specify which contract]  [ ] Compliance with a legal obligation [Please specify which legal obligation]  [ ] Vital interests of the data subject or another natural person [Please specify which]  [ ] Processing is necessary to complete a task carried out in the public interest or in the exercise of official authority which you have been assigned with [Please specify which public interest/public exercise of authority]  [ ] Balancing of interests in relation to your company’s legitimate interests balanced against the interests of the data subject [Please specify on the interest that you follow by processing data]  [ ] (Collective) agreements [Please specify which (collective) agreement]  [ ] Special legislation [Please specify] |
|  | 1. What is the basis for the collection and processing of the special categories of personal data? | [ ] Explicit consent [Please specify how consent is given and what it covers]  [ ] Meeting your legal obligations in the field of employment and social security and social protection law [Please specify which]  [ ] Vital interests for the data subject or another natural person, where the data subject is physically or legally incapable of giving consent [Please specify which]  [ ] Personal data are manifestly made public by the data subject  [ ] Vital interests of the data subject or another natural person, where the data subject is physically or legally incapable of giving consent [Please specify which]  [ ] Processing is necessary for the establishment, exercise or defence of legal claims  [ ] Processing is necessary for reasons of substantial public interest on the basis of special legislation [Please specify which special legislation]  [ ] Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of special legislation [Please specify which special legislation]  [ ] Processing is necessary for reasons of public interest in the area of public health on the basis of special legislation [Please specify which special legislation]  [ ] Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes on the basis of special legislation [Please specify which special legislation]  [ ] Other special legislation [Please specify which special legislation]  [ ] (Collective) agreements [Please specify which (collective) agreement] |
| **Profiling** | 1. Do you make decisions based solely on automated (machine) processing of the personal data, including profiling (analyses on or predictions of personal aspects such as performance at work, financial situation, health, personal preferences, interests, behaviour, geographic location). | [ ] Yes *(further examination necessary to assess lawfulness)*  [ ] No |
| **Disclosure to third parties** | 1. Do you disclose data to third parties, either within or outside the group?   E.g. other group companies, public authorities, trade unions, potential employers, pension funds, etc. Please note that the question only relates to disclosure to third parties that are new independent data controllers (and not data processors) | [ ] Yes  a. Which category of recipients? [Recipient]  b. The recipient’s country: [Country]  c. Which personal data are disclosed to third parties? [Personal data]  d. Please describe the purpose of the disclosure: [The purpose]  e. How are the personal data disclosed? [Method of disclosure]  *Copy the text above and paste below if more than one recipient.*  [ ] No |
| 1. What is the legal basis for the disclosure of the personal data? | [Recipient]  [ ] Consent [Please specify how consent is given and what it covers]  [ ] Other basis for disclosure   * Ordinary personal data: [Please specify which data and which basis for disclosure] * Special categories of personal data: [Please specify which data and which basis for disclosure]   *Copy the text above and paste below if more than one recipient* |
| **Source** | 1. Where did you obtain the personal data? E.g. directly from the data subject, cookies, monitoring, web portals, applications, former employees, etc. |  |
| **Transparency** | 1. Did you notify the data subject that you are processing their personal data? E.g. in a privacy policy, employment contract or by intranet message or the like? | [ ] Yes  [ ] No |

# Section 3 – Data processors

|  |  |  |
| --- | --- | --- |
| **Subject** | **Question** |  |
| **Data processors** | 1. Do you use data processors in this process?   E.g. a recruitment consultant, salary management agency, digital marketing agency or a system supplier (e.g. hosting, cloud). | [ ] Yes  *Please complete the rest of section 3 of the questionnaire*  [ ] No |
| 1. Please list the following information for each data processor | a. Name of data processor: [name] (company, organisation, authority) and country: [country]  b. The role of the data processor/tasks relating to the processing (e.g. system access, software development, etc.): [role/tasks]  c. Which personal data are processed by the data processor? [personal data]  *Copy the text above and paste below if more than one data processor* |
| **Written agreement** | 1. Has a written agreement been entered into with the data processor regarding the processing of the data, confidentiality, technical requirements, liability etc. (a data processing agreement)? | [Name of data processor]  [ ] Yes  *If your answer is yes, this subject must be further examined*  [ ] No  *Copy the text above and paste below if more than one data processor* |
| **Countries outside the EU/EEA** | 1. Are any of the data processors located in (and your data disclosed to) countries outside the EU/EEA? | [ ] Yes [Please specify which data processors]  *If your answer is yes, this subject must be further examined*  [ ] No |

# Del 4 – Situations in which you are data processor for another company or public authority

|  |  |  |
| --- | --- | --- |
| **Subject** | **Question** |  |
| **Data controller** | 1. Who are the data controller(s) for whom you process the data?   Please describe concrete companies or categories |  |
| **Processing and purposes** | 1. Please describe how and why you process personal data on behalf of the data controller(s). |  |
| **Own purposes?** | 1. Do you make individual decisions on the processing of the personal data or does the processing take place solely on basis of instructions from the data controller? | [ ] Yes   * Please describe the decisions and the purposes relating to your processing of: [Decisions and purposes]   [ ] No |
| **Written agreement** | 1. Did you (as data processor) enter into a written agreement with the data controller on the processing? E.g. on data processing, confidentiality, technical requirements, liability etc. | [ ] Yes  [ ] No  *Copy the text above and paste below if more than one data controller* |
| **Sub-processors** | 1. Do you provide access to personal data to sub-processors, e.g. a hosting-provider, web service or remote helpdesk? | [Name of sub-processor]  [ ] Yes [please specify]  a. Name of sub-processor: [name] (company, organisation, authority) and country: [country]  b. The role of the sub-processor/tasks relating to the processing: [role/tasks]  *Copy the text above and paste below if more than one sub-processor.*  [ ] No |
| **Sub-processor agreements** | 1. Has a written agreement on processing, confidentiality, technical requirements etc. been entered into with the sub-processor? | [Name of sub-processor]  [ ] Yes  [ ] No  *Copy the text above and paste below if more than one sub-processor* |
| **Countries outside the EU/EEA** | 1. Are any of the sub-processors located (and your data transferred to) countries outside the EU/EEA? | [ ] Yes  *If your answer is yes, this subject must be further examined*  [ ] No |

# Del 5 – General compliance

|  |  |  |
| --- | --- | --- |
| **Subject** | **Question** |  |
| **Requests from data subjects** | 1. Do you have internal guidelines or procedures for handling requests from data subjects?   E.g. if a data subject requests access to a copy of their personal data. | [ ] Yes  [ ] No |
| **General guidelines and training** | 1. Do you have internal guidelines or training concerning the processing of personal data included in this dataflow?   That is, which personal data may be collected, for which purposes, who may the data be disclosed to, etc. | [ ] Yes  [ ] No |
| **Personal data breaches** | 1. Do you have procedures to identify and handle personal data breaches?   Personal data breaches include everything from loss of USB-keys, loss of computer, loss of external hard drive, loss of backup, hacker attacks, etc. | [ ] Yes  [ ] No |
| Do you keep a log or a record of personal data breaches? | [ ] Yes  [ ] No |