

2018-05-28

**How to register a processing of personal data**

***KI GDPR***

**Dokumenthantering**

Detta dokument är aktuellt vid aktuellt datum då dokumentet producerades eller senast uppdaterades. Dokument med historik finns sparad under projektets arbetsmapp i KI Share: GDPR 🡪 Interna dokument 🡪 Delprojekt 🡪 Kartläggning

**Revisionshistorik**

Dokumentet har ändrats enligt följande:

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Version nr** | **Kommentar** | **Reviderad av** |
| 2018-03-15 | 0.1 | Upprättande av dokument | Lukas Grönquist |
| 2018-03-16 | 0.2 | Revidering och anpassning av exempel för KI | Lukas Grönquist |
| 2018-03-20 | 0.3 | Revidering efter återkoppling från projektgruppen | Lukas Grönquist |
| 2018-05-28 | 0.4 | Revidering efter färdigställande av anmälningsformuläret | Lukas Grönquist |
| 2018-07-01 | 0.4 | Översättning | Lukas Grönquist |

**Godkännande historik**

Detta dokument godkänns enligt följande:

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Version nr** | **Godkänd av** | **Titel** |
|  |  |  |  |
|  |  |  |  |

**Bilagor**

Detta dokument har följande bilagor kopplade till sig:

|  |  |
| --- | --- |
| **Nr** | **Beskrivning** |
|  |  |

**Table of Contents**

[1 Inledning 1](#_Toc517790735)

[Begrepp och definitioner i dokumentet 1](#_Toc517790736)

[2 Instruktioner för kartläggningsmallen 2](#_Toc517790737)

# Introduction

One of the requirements in GDPR is that KI needs to keep a record over the processing activities regarding personal data that is being done at KI. Therefore, all processing activities needs to be reported through the form that can be found at the following link [[http://registeranmalan.ki.se](http://registeranmalan.ki.se/)]. The registration of processing activities will be done in different ways depending on your area of ​​work, see the sections below for more detailed information.

**Research:**  
All research group leaders at KI must report the processing activities that is being carried out by their research group.

**Education and Administration:**  
If you work with education or administration at KI, you will only need to register processing activities that is being done outside of KI central systems. Although, this only applies if the activity is planned to last for more than three months. [Here is a link to the KI central systems](https://ki.se/sites/default/files/2018/06/28/forteckning_ki_gemensamma_system_0.2.docx).

This document provides guidance on how to register a processing activity at KI. Several of the fields in the form at the website have tooltips that contains similar information to these instruction, in order to display the tooltips, hoover your cursor over the question mark to the right of the question (?).

## Definitions

|  |  |
| --- | --- |
| **Word** | **Definition** |
| KI | Karolinska Institutet |
| GDPR | General Data Protection Regulation |
| Personal data | Personal data means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person |
| Processing | Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; |

# Instructions

|  |  |  |
| --- | --- | --- |
| # | Question | Instructions |
| 1 | Contact person for the processing activity at the department. | The contact person is the one who is responsible for the processing at KI, you will need the enter at least the following information:  - First name  - Last name  - Phone number  - Email  - Institution or equivalent  - Field of work  This may be used for future follow-up of the registered processing activity. |
| 2 | The name of the processing activity | A *processing activity* is an operation or a set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.  It can be difficult to distinguish one processing from another. An advice is to follow the structure and names in systems or business processes as closely as possible. You can also collect processing activities that is similar to each other, has the same purpose, concerns similar categories of personal data, is being done in the same IT-systems into one processing activity and report it as one processing.  If there are multiple processing activities within the same system or business process, you should name them differently. |
| 3 | Is there another party than KI that is the controller of the processing | If KI has determined the purpose and means for the processing of personal data, KI is the controller of the processing and you shall enter (Nej/No).  If there is another party who has determined the purpose and the means of the processing, then it is that party who is the controller and you shall enter (Ja/Yes). (Ja/Yes) should also be entered in cases where you have determined the purposes and means for the processing together with another party.  In the field *Vem/vilka är personuppgiftsansvarig*, the controller of the processing shall be entered (not applicable when KI are the processor).  In the field *Diarienummer på avtalet som reglerar behandlingen* the registration number of the agreement that regulates the processing of personal data shall be entered. This usually is a data processing agreement (DPA). |
| 4 | IT-systems that is being used | Specify which IT-systems that is being used for the processing. Examples of systems are:  - KI Box  - KI Share  - Primula - KI ELN  - SPSS  One processing activity can include multiple systems, usually one system is used for storage while another system is used for the processing of personal data. If multiple systems are being used these should be listed here. To enter multiple systems manually, select (Annat) and specify the systems that are being used separated by a comma (,). |
| 5 | Purpose of the processing | When describing the purpose of the processing, enter an explicit purpose and be specific in the description.  Example of a purpose:  - For a HR-system, the purpose could be "Processing of employee information for employee management, planning and monitoring, and also to manage personnel duties".  The description should rather be too detailed in the description than too briefly, it should be clear why personal data need to be processed and what the purpose of the processing is. |
| 6 | Categories of data subjects | Select which categories of data subjects that are subject to the processing. Data subjects are those who get their personal data processed, e.g. employees at KI, affiliated, students at KI, postgraduate students, patients (not researchers), researchers, jobseekers or others. |
| 7 | Estimated number of data subject that are affected by the processing | Here you will have to enter an approximate number of data subjects that are affected by the treatment. |
| 8 | The processing includes the following categories of personal data | Here you’ll need to enter what categories of personal data that are being registered and processed.  Example:  - For payroll administration: Name, social security number, address and income details.  - For research: Age, gender, health data and biological samples. |
| 9 | What source is used for the collection of personal data? | Directly from the data subject is often the collection is being done through questionnaire or interviews.  If you collect the personal data from another source the data subject, you’ll need to specify from which source. |
| 10 | Has or will personal data be transferred outside of KI. Transfer to third countries shall not be entered here, it will be done in the next question. | Here you will need to enter if there are any recipients of the personal data that is being processed. As an example, if personal data will be transferred to County Council, CSN, other universities or companies, etc. If the personal data have or will be transferred to another party, you also need to specify by which means the transfer will be made.  This questions only includes external recipients, recipients within KI shall not be specified (for example, transfer within your or another institutions).  Recipient - "A natural or legal person, public authority, agency or other body to which personal data are disclosed". |
| 11 | Has or will personal data be transferred to a third country (country outside of EU/EEA) | If personal data will be transferred to a third country, this or these countries will need to be entered here.  EU countries: Belgium, Bulgaria, Cyprus, Denmark, Estonia, Finland, France, Greece, Ireland, Italy, Croatia, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, United Kingdom, Sweden, Czech Republic, Germany, Hungary, Austria.  EEA countries: Iceland, Liechtenstein, Norway |
| 12 | How long will the personal data will be processed before deletion | To answer this question, an analysis of how long the personal data will be processed in an identifiable form is required.  The time intervals in this question are taken from KI’s document management plan, which should be used to answer this question. |
| 13 | Which lawful basis is used for processing | Enter which lawful basis that is being used for the processing of personal data. In GDPR the following lawful bases are mentioned:  - Consent  - Performance of a contract  - For compliance of a lawful obligation  - To protect vital interests of the data subject  - Public interest or as an exercise of official authority vested in the controller  - Legitimate interest  Research and education at KI goes under the lawful basis of “Public interest or as an exercise of official authority vested in the controller”. Other business areas at KI may use one of the other lawful bases (with restrictions for legitimate interest) |
| 14 | Enter the measures that has been implemented to increase the security of the personal data | If possible, describe the technical and organizational security measures that has been implemented to increase the security of the personal data.  It is not a requirement to describe these measures in detail, but you should give a brief description or refer to the security measures if these are documented elsewhere. Contact the IT-department if you have any questions about the security of systems provided by them. |
| 15 | Are there any processors for the processing of personal data | If there is a natural or legal person, public authority, institution or other body that processes personal data on behalf of KI, this should be stated (Ja/Yes).  A reference to the Data Processor Agreement must be made here by entering the registration number of the agreement.  Examples of situations when the processing can include a processor:  - KI stores personal data on a cloud service  - KI sends biological samples to another university or company for analysis  - KI sends records containing personal data to other universities or companies for processing of the records  - External persons are staying and processing personal data at KI with KI's technical equipment. |
| 16 | Is there approval for research from the Ethical Review Board (only for research at KI) | Research requires that there is an approval for the research from the Ethical Review Board. Here, KI's registration number for the approval should be entered. |