# List of Data Processing Activities

This template is supposed to give you an idea of the structure. Don’t use word - this is thought as an excel / sheets file. Think of the sub-sections below as different tabs in your excel sheet.

Disclaimer: data privacy documentation should usually be written in the official language of your EU member state. Most likely, you should translate this template accordingly. In German, people refer to this typically as the ‘Verzeichnis der Verarbeitungstätigkeiten’…

## Data Processing Activities

Note that this tab should exist twice: one time for internal processing activities and one time for external ones. *Internal* processing refers to your internal data that third parties may process on your behalf (for example: your tax accountant, your cloud provider, providers of all the tools you use in your company). *External* processing refers to data of third parties that you process on their behalf (for example: customer data that is transferred to your servers to be analyzed by your brand-new AI algorithm).

***Categories:*** *ID - Controller - Controller Address - Controller Contact Details - Legal Basis - Processing Purpose - Category of Data - Data Subjects - Start Date of Processing - End Date of Processing - Processor - Processor Address - Processor Contact Details - Legal Basis - Threshold Analysis - DPIA - Description of TOMs - Deletion Period - Transfer to Third Countries - Safeguards - Commentary*

Consider that you will have a ton more data processing activities than categories. Write your categories as columns and processing activities as rows (the table in this template is transposed (rows and columns flipped) due to formatting reasons).

| Categories | Data Processing Example #1: Processing of Health Data by a Cloud Provider (Internal) | Data Processing Example #2: Processing of Applicant Data by a Software Tool Provider (Internal) | Data Processing Example #3: Processing of Health Data by Your Company as Clinical Decision-Support (External) | (…) |
| --- | --- | --- | --- | --- |
| ID | 1 | 2 | 3 |  |
| Controller | Example GmbH | Example GmbH | Berlin-Based Example Customer |  |
| Controller Address | Example Street 12310000 BerlinGermany | Example Street 12310000 BerlinGermany | (…) |  |
| Controller Contact Details | John Doejohn.doe@example.com | John Doejohn.doe@example.com | (…) |  |
| Legal Basis | Commissioned Data Processing(Art. 6 Sect. 1 lit. b) GDPR) | Pre-Contractual Measures(Art. 6 Sect. 1 lit. b) GDPR) | Commissioned Data Processing(Art. 6 Sect. 1 lit. b) GDPR) |  |
| Processing Purpose | Provision of Cloud Services | Management of Applicant Data | Provision of Decision-Support for Clinical Diagnoses |  |
| Category of Data | Patient Data (e.g. DICOM image data and clinical information) | Applicant Data (e.g. CV, cover letter, reference documents) | Patient Data (e.g. DICOM image data and clinical information) |  |
| Data Subjects | Patients that undergo CT lung cancer screening | Applicants to Example GmbH | Patients that undergo CT lung cancer screening |  |
| Start Date of Processing | 01.08.2021 | 01.01.2021 | 01.08.2021 |  |
| End Date of Processing | N/A | N/A | N/A |  |
| Processor | Berlin-Based Example Cloud Provider | California-Based Example Software Provider | Example GmbH |  |
| Processor Address | (…) | (…) | Example Street 12310000 BerlinGermany |  |
| Processor Contact Details | (…) | (…) | John Doejohn.doe@example.com |  |
| Legal Basis | Commissioned Data Processing (Art. 6 Sect. 1 lit. b) GDPR) | Commissioned Data Processing (Art. 6 Sect. 1 lit. b) GDPR) | Commissioned Data Processing (Art. 6 Sect. 1 lit. b) GDPR) |  |
| Threshold Analysis | Acceptable | Acceptable | N/A |  |
| DPIA | N/A | N/A | N/A |  |
| Description of TOMs | Entry Control: locked building, documented key assignment (..)Access Control: central password authentication incl. 2FA (…)Usage Control: role-based authorization (…)Availability: uninterrupted power supply, continuous backups (…)(…) | (…) | (…) |  |
| Deletion Period | 30 days after data ingestion | 6 months | 30 days after data ingestion |  |
| Transfer to Third Countries | No | United States of America (USA) | No |  |
| Safeguards | N/A | EU Model Contract Clauses | N/A |  |
| Comment |  | Note that after ECJ Schrems II ruling, model contract clauses alone are not sufficient to safeguard data transfer to the U.S. |  |  |

## Threshold Analysis and Data Protection Impact Assessment

Note that it is the responsibility of the controller to carry out a DPIA (Art. 35 GDPR)

Optionally, you can split this section into two separate tabs.

Reasoning: whenever a risk is deemed acceptable in a previous section, the documentation ends right there. For example, if the overall severity and probability of a risk are deemed acceptable, you don’t have to dive into further evaluation criteria of the next section or let alone start the DPIA for this risk. Sections are shown in the text below in brackets - use different formatting when you adopt this template).

As part of your DPIA, you typically analyze several risk causes. More risk examples are listed in the risk methodology section.

**Categories TA:** *(Risk Identification) - Processor - Processing Purpose - Risk Cause - Risk Description - (Initial Risk Assessment) - Severity - Probability - Assessment - (Further Evaluation Criteria: Special Processing) - Processing large quantities of personal data - Processing affects a large number of people - Use of new technologies - Processing hampers the exertion of data subject rights - Processing hampers the use of services or exertion of contracts for data subjects - Processing of data of vulnerable persons - (Further Evaluation Criteria: Automated Decision-Making) - By systematic assessment of personal characteristics based on profiling - By processing special categories of personal data - (Responsible data protection authority deemed processing high-risk)*

**Categories DPIA:** *Planned additional measures - (Re-Evaluation) - Severity after measures - Probability after measures - New assessment - (Implementation) - Responsible - Status - Date of Implementation - Notification of Authorities*

| Categories | Data Processing Example #1: Processing of Health Data by a Cloud Provider (Internal) | Data Processing Example #2: Processing of Applicant Data by a Software Tool Provider (Internal) | (…) |
| --- | --- | --- | --- |
| ***Threshold Analysis*** | - | - | - |
| ***Risk Identification*** | - | - | - |
| Processor | Berlin-Based Example Cloud Provider | California-Based Example Software Provider |  |
| Processing Purpose | Provision of Cloud Services | Management of Applicant Data |  |
| Risk Cause | Unauthorized access | Unauthorized access |  |
| Risk Description | Sensitive patient data could be identified by third-parties, leading to a risk of identity theft | Applicant data could be identified by third-parties, leading to a risk of identity theft |  |
| ***Initial Risk Assessment*** | - | - | - |
| Severity | S4 | S3 |  |
| Probability | P2 | P2 |  |
| Assessment | Unacceptable | Acceptable |  |
| ***Further Criteria: Special Processing*** | - | - | - |
| Processing large quantities of personal data | No | - |  |
| Processing affects large numbers of people | No | - |  |
| Use of new technologies | No | - |  |
| Processing hampers the exertion of data subject rights | No | - |  |
| Processing hampers the use of services or exertion of contracts for data subjects | No | - |  |
| Processing of data of vulnerable persons | No | - |  |
| ***Further Criteria: Automated Decision-Making (ADM)*** | - | - | - |
| ADM by systematic assessment of personal characteristics based on profiling | No | - |  |
| ADM by processing special categories of personal data | No | - |  |
| *Responsible Data Protection Authority deems processing high-risk* | No | - |  |
| ***Data Protection Impact Assessment*** | - | - | - |
| Planned additional measures | - | - |  |
| ***Re-Evaluation*** | - | - | - |
| Severity after measures | - | - |  |
| Probability after measures | - | - |  |
| New assessment after measures | - | - |  |
| ***Implementation*** | - | - | - |
| Responsible Role | - | - |  |
| Status of Implementation | - | - |  |
| Date of Implementation | - | - |  |
| Notification to Authorities | - | - |  |
| Comment |  |  |  |

## Risk Methodology

This field should provide the taxonomy and an overview of the possible categories of content entered in the previous tabs.

**Possible categories of risk:**

* Data loss (availability)
* Unauthorized access (confidentiality)
* Unauthorized modification (integrity)
* Non-compliance (e.g. not deleting data)

**Categories of data processed by the company:**

* Employee data
* Customer data (of commercial partners)
* User data (of employees of partners)
* Patient data

| Degree of Severity | Social Damage (e.g. discrimination, loss of reputation) | Financial Damage | Identity theft | Mortal Danger | Disclosure of Secrets |
| --- | --- | --- | --- | --- | --- |
| S1: Low | No or minor societal or economical disadvantages in daily life | In the scope of a one month salary |  |  |  |
| S2: Rather Low | Societal or economical disadvantages can be noticed and lead to minor restrictions in daily life | In the scope of several months of salary |  |  |  |
| S3: Rather high | Implications for an entire part of daily life for a person affected (e.g. work place / professional environment) | In the scope an annual salary |  |  | Disclosure of secrets has implications for a part of life of a person affected |
| S4: High | Major disadvantages for an affected person across all fields of life (e.g. job loss or implications for personal surrounding) | Loss of all financial means | Identity theft | Mortal danger | Geheimnisoffenbarung hat Auswirkungen auf das gesamte Leben des Betroffenen. |

| Probability of Occurrence | Future Estimate | Past Estimate |
| --- | --- | --- |
| P1: Never | Event is unimaginable | Event has never occurred |
| P2: Seldom | Event may on average occur once every 10 years | Event has never occurred or more than 10 years ago |
| P3: Rather unlikely | Event may on average occur every 5-10 years | Event has occurred in the last 5-10 years |
| P4: Rather likely | Event may on average occur every 1-5 years | Event has occurred in the last 1-5 years |
| P5: Frequently | Event occurs at least once per year | Event has occurred in the last year |

Note: fields that are marked red symbolize a combined severity and probability that is unacceptable, yellow fields are acceptable.

|  | S1: Low | S2: Rather Low | S3: Rather High | S4: High |
| --- | --- | --- | --- | --- |
| P5: Frequently | S1P5 (yellow) | S2P5 (red) | S3P5 (red) | S4P5 (red) |
| P4: Rather likely | S1P4 (yellow | S2P4 (red) | S3P4 (red) | S4P4 (red) |
| P3: Rather unlikely | S1P3 (yellow) | S2P3 (yellow) | S3P3 (red) | S3P3 (red) |
| P2: Seldom | S1P2 (yellow) | S2P2 (yellow) | S3P2 (yellow) | S4P2 (red) |
| P1: Never | S1P1 (yellow) | S2P1 (yellow) | S3P1 (yellow) | S4P1 (yellow) |

Template Copyright [openregulatory.com](https://openregulatory.com). See [template license](https://openregulatory.com/template-license).

Please don’t remove this notice even if you’ve modified contents of this template.