RKG: New Systems Guidelines / Data Protection Impact Assessments

A. Introduction

RKG is committed to protecting the personal data of our employees, customers and business partners, which is why we have adopted the 10 Data Protection Principles set out in our *Data Protection Policy*.

Our *Data Protection Policy* requires RKG to conduct a careful assessment of data protection requirements when introducing or substantially changing data processing, in particular when planning to introduce new systems. This process requires to pay attention to various aspects, namely to assess all risks potentially involved with the processing of personal data. This risk assessment is required (i) to determine appropriate technical and organizational measures (Art. 24, 32 GDPR), (ii) to act in accordance with the requirements for data protection by design and by default (Art. 25 GDPR), and (iii) for a "**Data Protection Impact Assessment**" (also known as a "**DPIA**", Art. 35, 36 GDPR) where there are likely to be high risks associated with any new processing of personal data.

"**Personal data**" means information which relates to an identified or identifiable individual (i.e. a natural person). It includes names, addresses, email addresses, job applications, photographs, purchase histories, user account information, and correspondence to and from an individual. Where it can be linked to an individual, it also includes web browsing information (e.g. cookie data).

These Guidelines explains what a risk assessment, data protection by design, and a DPIA is, the circumstances when a DPIA must be conducted, and how to conduct one.

PART 1 of these Guidelines apply to **all RKG staff**. It sets out the triggers for when you will need to discuss any new project with your Managing Director of RKG, who will then decide whether or not a full DPIA is necessary.

PART 2 of these Guidelines apply only to Managing Director of RKG, who will have responsibility for conducting the DPIA.

PART 1: APPLICABLE TO ALL STAFF

1. What is a Risk Assessment and a Data Protection Impact Assessment (or "DPIA")?

A risk assessment is an assessment of the impact on individuals of the processing of their personal data. Conducting a risk assessment enables RKG to decide whether it is justified in conducting a particular data processing activity, and determine how to do it in the most 'privacy friendly' manner. On this basis RKG needs to determine appropriate safeguards, how to implement the most data protection friendly tools and instruments and which technical and organisational measures are necessary and adequate. A DPIA is a more formal process to do this in cases where RKG must take more precautions than usually.

The risk assessment and the DPIA in particular works by making RKG identify the benefits of a proposed project, the possible privacy and data protection risks, and any safeguards which can be put in place to mitigate those risks. Whoever is conducting the risk assessment or the DPIA can then decide whether the project can go ahead, or whether any further mitigation steps are needed.

All staff have a responsibility to assist with a risk assessment in every case new systems are introduced or in case of changes to an existing system, and to assist with a DPIA if asked to do so by the Managing Director of RKG. The Managing Director of RKG will need to know details of the project, including about the business case and proposed technology, and so your co-operation is critical.

2. What are the risks of a processing and do you think the processing <u>might be</u> high risk?

While an assessment of risks is always required, a DPIA is required only where any processing of personal data **is likely** to result in a '**high risk**' to the rights and freedoms of individuals. The Managing Director of RKG will decide whether a DPIA is required in any case.

As an important first step, however, any new processing requires a risk assessment and a processing which has the **potential** to be high risk should be referred to the Managing Director of RKG. The Managing Director of RKG will then decide whether or not to conduct a full DPIA.

The following processing activities should be referred to the Managing Director of RKG, because there is a likelihood of high risk. If the proposed activity is similar to or the same as the list below, you should also refer it to the Managing Director of RKG. In other cases, you may simply use your assessment to determine adequate safeguards and data protection friendly steps and tools.

However note these are examples of "risk triggers" and this is <u>not</u> an exhaustive list. Any substantial new use of personal data has the potential to be high risk.

Processing Activity	**Example**
Sharing a significant amount of personal data with a third party, including service providers	• Appointment of a new supplier who will have access to customer data
Collection of a new type of personal data	• Collecting photographs as part of a customer account sign-up
Collection of a new type of sensitive personal data, or using sensitive personal data for a new purpose "**Sensitive personal data**" is personal data relating to: • racial or ethnic origin • political opinions	• Allowing customers to add health information to their account • Collecting fingerprints for an app login

• religious or philosophical beliefs • trade union membership • biometrics • genetic information • mental/physical health • sex life or sexual orientation	
Using personal data for a new purpose	• Introducing a new way of personalising the service
Using personal data to make a decision about someone on an automated basis (even if there is a human review)	• Using an automated programme to assess CVs in recruitment
New collection or use of location data or payment card information	• Adding location tracking to an app
Collection of personal data about children under 16	• Introducing a new website aimed at children
Sharing sensitive personal data with a third party	• Appointing a third party service provider who will have access to employee occupational health data
Conducting monitoring of individuals	• Adopting a new CCTV system • Monitoring employee use of an IT system (e.g. keylogger software, email monitoring, drug testing) • Location tracking via an app
Any new profiling of individuals, that is, using personal data to evaluate or draw conclusions about their interests, behaviour or circumstances	• Using web browsing activity or other customer interactions to assess a customer's social circumstances (purchasing power, family status etc.) for marketing purposes
Combining datasets previously maintained separately	• Combining data across Brands for the first time
Transferring personal data outside the EEA, other than as part of an existing processing arrangement already in place	• Appointing a US service provider (e.g. a cloud provider or offshore call centre)

If you are still not sure, you should speak to the Managing Director of RKG.

The following are examples of processing which are unlikely to be high risk, and in the absence of special circumstances would not require a DPIA (but still you need to determine adequate safeguards and data protection friendly steps and tools):

- ‘Business as usual’ processing which RKG has been engaged in for several years, such HR administration and email marketing, provided there is no material change in the processing.
- Ad hoc processing of a small amount of personal data in response to a specific request by the data subject (e.g. in the context of a customer query).
- Disclosure or other processing of staff business contact details.

PART 2: APPLICABLE TO THE MANAGING DIRECTOR OF RKG ONLY FOR DPIA

1. Is the processing 'high risk'?

The next step is for the Managing Director of RKG to decide whether it is necessary to conduct a DPIA, on the basis that the processing **is likely to pose a high risk** to the rights and freedoms of individuals. This is an initial assessment to determine if a DPIA is required.

The Managing Director of RKG will need to understand the key details of the proposed processing in order to make this initial assessment. As a minimum you will need to understand:

- the nature of the data and the data subjects;
- the nature, scope and context of the processing;
- the purpose of the processing; and
- the identities of the parties involved.

It is **mandatory** to complete a DPIA in the following circumstances:

- Making 'automated decisions' (i.e. decisions made solely on an automated basis, with no human intervention), which have more than a trivial impact on individuals and are based on profiling or some other systematic evaluation of the individual's behaviour, e.g. online tracking or geo-location data.
- Processing sensitive personal data on a 'large scale'. Processing will be 'large scale' if it concerns a substantial portion of employees or customers, and/or if it concerns a large amount of data (even if only about a small number of individuals).
- Monitoring a public area (other than on a one-off basis).
- In any one of the cases defined by German data protection authorities as "must" cases of a DPIA.

Other than in the above cases, it will be up to you to exercise your judgment. Looking at all the facts, do you think the project is likely to pose a high risk to individuals? If, having considered the key details of the proposed processing you are satisfied that the proposed processing is not likely to pose a high risk to the rights and freedoms of individuals, you will not need to conduct a DPIA. If you are unsure, you should conduct a DPIA (although this could be a shorter DPIA), as this will assist in clarifying your understanding of the risks involved.

2. Conducting the DPIA

The DPIA will need to be recorded in a way which captures all of the steps below. There is a template form for you to use at **Annex 1**.

Note that although you should always complete all the steps, each DPIA will not always require the same level of detail. The extent of the DPIA will depend on the nature of the project and risks involved. If it is a straightforward project, and perhaps you were unsure as to whether a DPIA was needed, the DPIA can be relatively short. In contrast, a larger, or more complicated, or more obviously 'risky' proposal will likely require a more thorough DPIA.

Step (1): Create a description of the proposed processing, including:

- The nature of the personal data.
- The identity of the data subjects and (approximately) how many there will be.
- The nature of the processing (i.e. what will be done to the personal data).
- The purpose and business objectives of the processing (i.e. why it has been proposed).
- The identity and location of the parties, particularly if any are outside the EEA.

You will need to speak to those involved in the project, which may include the business owner, system owners, project managers, procurement and IT.

Step (2): Identify why there was a need for a DPIA (i.e. why is the processing likely to be high risk). Essentially, you should explain your decision to conduct a DPIA.

Step (3): Identify the legal basis for the processing under data protection law.

In most cases this will be **one** of the following:

- That RKG will obtain the individual's freely given, informed **consent**. If the data is sensitive personal data, this consent must be **explicit.**
- That the processing is **necessary for the performance of a contract** with the individual (or pre-contractual steps).
- That the processing is necessary for RKG's **legitimate interests**, which are not outweighed by any prejudice to the individuals. If RKG is relying on this basis, you must also specify the legitimate interest (e.g. increased customer insight). You cannot rely on this basis to process sensitive personal data.

Identifying the legal basis will help you understand the privacy risks and how to protect against them. If the individuals have a genuine choice as to whether their personal data is processed for the project (and so RKG can rely on consent), you may be able to accept a higher level of risk to those individuals than if they have no choice.

Step (4): Identify the key privacy risks i.e. the risks to the rights and freedoms of the data subjects.

You should consider the potential threats arising from the process. Examples might include:

- RKG having less control over how the personal data is used.
- Use or storage of inaccurate or out-of-date data.
- Unjustifiable or excessive collection of data.
- Inappropriate use or misuse of data.
- Destruction or alteration of data.

- An increased risk of a hack or security breach.

You should then consider the likelihood and severity of any harm that might result from the processing. Examples might include:

- Identity theft, discrimination, financial fraud, or simply exposing sensitive details about people if the information was made public.
- Complaints or upset from individuals.

You should also capture any related commercial or legal risks to RKG, such as:

- Damage to our customer relationships.
- Increased risk of investigation and/or penalties by the ICO.
- Risk of negative media attention.

Step (5): Identify the necessary safeguards which should be put in place to address the risks you identified at Step 4.

This will require you to consult with the relevant stakeholders to ensure the proposed safeguards are commercially viable.

Examples of the sorts of privacy safeguards you should consider include:

- Putting in place appropriate security measures, e.g. encryption, access controls, firewalls, cybersecurity measures, physical security measures.
- Considering whether the data can be pseudonymised or anonymised.
- Ensuring transparency to the data subjects – does RKG need to amend its Privacy Policy or create a new notice?
- Implementing a 'privacy by design' approach – how can the solution be designed to address privacy concerns?
- Considering offering an 'opt-out' or consent-based approach.
- Ensuring robust contractual protections are put in place with third parties.
- Ensuring there are set retention periods for the data, after which it is deleted or anonymised.

Note that you do not necessarily need to eliminate the risks completely; the critical point is to minimise the risk to the greatest extent reasonably possible.

Step (6): Assess the necessity and proportionality of the processing, in view of the purpose it is intended to achieve.

Consider why RKG needs to conduct the processing, and whether there is any less impactful method which could be used instead. Points to consider include:

- What are the benefits to stakeholders, including the data subjects or RKG? Are they sufficient to justify the risks?
- Could we achieve the same outcome with anonymous information?

CRITICAL STEP: Can the project go ahead?

At this stage, you may decide that the risks associated with the project mean it should not go ahead in its current form. If RKG cannot put in place sufficient safeguards to mitigate any privacy risks, it has an obligation to consult with the responsible data protection authority and – ultimately – the project may not be able to go ahead.

You should consult Managing director of RIKEN KEIKI GmbH and Administration team of RIKEN KEIKI Co. Ltd. if you do not think the privacy risks can be adequately mitigated, and the project remains '**high risk**'.

Step (7): Identify the action items necessary to implement each safeguard.

You should assign an owner for each item and set milestone(s) for its implementation. This should be done in consultation with the relevant stakeholders.

Step (8): Check the record of the DPIA accurately captures all the details of your assessment and the outcome.

You should then send a copy to Managing director of RIKEN KEIKI GmbH and Administration team of RIKEN KEIKI Co. Ltd., to be maintained in a central register.

Last updated [•]

ANNEX 1: DPIA TEMPLATE
DATA PROTECTION IMPACT ASSESSMENT

PROJECT NAME:

RESPONSIBLE: Managing Director of RKG

DATE DPIA COMPLETED:

STEP (1): A DESCRIPTION OF THE PROCESSING
STEP (2): WHY IS THERE A NEED FOR A DPIA?
STEP (3): WHAT IS THE LEGAL BASIS FOR THE PROCESSING?
STEP (4): WHAT ARE THE RISKS?
STEP (5): IS IT NECESSARY AND PROPORTIONATE?
[CONSULTATION WITH MANAGING DIRECTOR OF RIKEN KEIKI GmbH AND ADMINISTRATION TEAM OF RIKEN KEIKI CO. LTD AND/OR THE DATA PROTECTION AUTHORITY]
[DELETE IF NOT APPLICABLE]
STEP (6): SAFEGUARDS
STEP (7): ACTIONS

Provide a copy of the completed DPIA to Managing director of RIKEN KEIKI GmbH and Administration team of RIKEN KEIKI Co. Ltd.