

RKG: Individual Rights Guidance

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

Principle 8 is “Individual Rights”: RKG will allow individuals the right to access, correct or erase their personal data, or object to it being used for certain purposes. These Guidelines are designed to help you apply Principle 8 in practice.

1. Who do these Guidelines apply to?

These Guidelines outline steps that must be followed in the event we receive a rights request (as further described below). The steps in Part 1 of these Guidelines applies to **all** RKG staff.

The steps in Part 2 applies **only to Administration and Sales**, who will have responsibility for performing the relevant actions as further specified in the relevant steps below.

Any staff who fail to comply with this Policy may be subject to disciplinary action, up to and including dismissal.

If you have any questions about this Policy, you should contact Administration team of RIKEN KEIKI GmbH through its website.

2. What is a rights request?

Under data protection law, individuals have certain rights in respect of their personal data. These are:

- (i) **Access:** The right to know what personal data RKG processes about them, and to obtain a copy of that personal data. In some cases, we may need to provide this copy in a machine-readable format which the individual could share with another organisation (this is known as “data portability”).
- (ii) **Rectification:** The right to have inaccurate data corrected (and/or incomplete data completed with supplementary data).
- (iii) **Erasure:** Sometimes known as a “right to be forgotten”, the right to have personal data erased when RKG has no lawful basis to continue processing the data. In some cases, we might not erase the data completely but instead just restrict its use (e.g. so it can only be used to defend us in the event of a legal claim).
- (iv) **Objection:** Individuals have the right to object to their personal data being used for a particular purpose, e.g. to send them direct marketing, customer profiling, or making entirely automated decisions which significantly affect them.

All of these are known as “rights requests”. Broadly speaking, any request by an individual regarding their personal data is a rights request. This includes where the request is received via phone, email, letter, or even social media. It does not have to mention data protection law or personal data. However, rights requests should not be

confused with normal, day-to-day customer service queries about a customer's *account* (e.g. asking why their order has not arrived).

The standard for whether RKG has to comply with the request varies depending on which right is being exercised. In some cases, the individual may be seeking to exercise more than one right, and so we may be able to comply with one aspect of a request (e.g. granting access), but not another (e.g. erasure).

RKG must respond to rights requests within **one month**. If the request is particularly complicated, we can extend this to **two months**, but we must still respond to the requestor within one month, explaining why we need the extension.

Note that we are not entitled to charge a fee for dealing with requests, other than in exceptional circumstances, such as where we have already provided the information to the individual.

Part 1: Applicable to all RKG Staff

Steps to be taken in the event a rights request is received

Step 1 – Confirm the identity the requestor

Before taking any action in relation to a rights request, we must be sure that it comes from the person whom the personal data is about (known as the “data subject”), or someone authorised to act on their behalf.

There are a variety of ways to identify the requestor's identity, such as asking for information only the account holder would know (e.g. their last two orders), ringing the individual, asking for ID (such as driving licence) or asking for home address or phone number etc. We must not ask for more information than the minimum reasonably necessary to identify the requester. If the requestor is an employee, we may not need any additional information to verify their identity.

Oral Requests

Rights request can be made orally (e.g. to a call centre or in person). If the request was received orally, we should ask the requestor if they will put the request in writing (e.g. by sending an email). We cannot insist on this, and we cannot refuse to respond to requests which are only made orally. However, you should explain to the requestor that it is easier for us to respond to written requests, and so may mean the response is dealt with more quickly.

If the individual refused to put their request in writing, RKG should send the individual a written communication as soon as possible confirming the nature and scope of their request.

Resolving request ‘informally’

Often, where a request is very simple, it may be easier to assist the requestor on a more informal basis without having to follow the procedure set out in this Guidance. If it is possible to satisfy the requestor's query quickly, without escalating the matter further, it is more likely that RKG will be able to limit the scope of the request. Formal rights requests place a greater

burden on RKG in terms of resources, and also expose us to a greater risk of regulatory complaints.

By way of a practical example, if a customer telephones our call centre and requests a copy of a single email which he/she has previously sent or received but has accidentally deleted, it is preferable for customer service to simply re-send the email (provided we are certain they are who they say they are). By escalating the request to a formal process, there is a significant risk that the individual will broaden the scope of their request (for example, seeking copies of “all communications”). This is clearly a far more onerous request for RKG to comply with.

Consequently, wherever possible attempts should be made to comply with informal requests and avoid them turning into formal rights request.

Rectification Requests

As a general rule, it should be possible to resolve Rectification requests at an informal stage. We can either do this by correcting the original record or adding a supplementary statement to the record.

For example, we frequently receive requests to change a customer’s address or name, if there is an error or they have moved house or got married. Provided we can verify the requestor’s identity, it should be possible to satisfy the request without escalating it any further.

If you have any concerns about a rectification request, you should pass the request to Managing director or Head of Administration team.

Step 2: Inform the correct RKG business units

If you receive a rights request you must immediately inform Managing director or Head of Administration team, even if you are still attempting to resolve the request informally. If the request relates to employment information, you should also inform Head of Administration team. If the request relates to information about any RKG customers, you should also inform Head of Sales team.

This includes where you have personally received the rights request or you have been told by someone else that they have received a rights request, such as where you have received a notification of a rights request from any of our suppliers or business partners.

Once you have informed the business units set out above, the following steps in this guidance can be progressed by the relevant business units. It is therefore very important that you comply with this Part 1 and inform the relevant personnel as soon as possible in the event a rights request is received.

Part 2: Applicable only to Administration and Sales

Step 3 – Is the request clear?

The next steps is for Managing director, Head of Administration team or Head of Sales team consider if the request contains sufficient information for us to be able understand and consider the request. Is sufficient for us to be able to find the information the individual is asking to access or erase. If it is too general/unclear, HR or Customer Services should ask the individual promptly for the additional information reasonably required to fulfil the request.

Step 4 - Identify the information

The next step is for HR or Customer Services to identify which RKG systems and databases may contain information relating to the individual and RKG business units which are responsible for those systems and databases.

This will depend on the nature of the information requested. However, it is likely that HR/Customer Services and the relevant business unit(s) will have to work with IT in order to identify the relevant RKG databases or systems that hold documents and information electronically.

The business units responsible for each such database and/or system will then need to carry out searches for any information which relates to the individual. Once these searches have been completed by the relevant business unit, that business unit should provide a copy of any information identified to HR or Customer Services for inspection.

Step 5 - Reviewing the information to identify personal data

Once the information has been provided to HR or Customer Services, they will need to review the information to identify any personal data which relates to the requestor. As a rule of thumb, you are attempting to identify information that is either biographical about the individual or which has the individual as its focus.

As part of this review, HR or Customer Services should also flag any/all information that RKG would **not** wish to disclose outside the company, for example, information that is commercially sensitive, embarrassing for RKG or critical of the individual or another person. It will then be for Managing director, Head of Administration team or Head of Sales team (in accordance with the steps below) to determine whether any such information may be withheld or redacted.

HR or Customer Services should then provide all of the reviewed information to Managing director, Head of Administration team or Head of Sales team.

Step 6 - Check for third party data

Once the reviewed information has been provided to Head of Administration team, he will conduct its own review of the information to determine whether the information includes information about other people.

We must not supply information about other people unless they have given their consent for the disclosure, or it is reasonable to supply the information without their consent. Following this review Managing director, Head of Administration team or Head of Sales team will decide if any such information should be withheld or redacted. If Head of Administration decides not to disclose the other people's information, we will still need to disclose as much information as possible by redacting the references to the other people.

Step 7 – Are we obliged to comply with the request (in whole or part)?

There are various legal exemptions which mean that we are not obliged to grant rights requests in respect of certain information, for example if it is legally privileged. National laws may also impose country-specific exemptions. Head of Administration should determine if any exemptions apply.

This will result in the creation of a subset of the information (or no information at all). For access requests, Head of Administration will provide this subset of the information back to HR or Customer Services as applicable so that it can be sent to the requestor.

Erasure and Objection Requests

The rights to erasure and objection are not absolute rights. RKG does not need to delete personal data which: (i) we need to retain to protect ourselves from legal claims (e.g. a contract, employment history, or correspondence with a customer about a product issue); (ii) we need to retain to comply with a legal obligation (e.g. for tax purposes); or (iii) which we need to retain to perform a contract with the individual.

Similarly, an individual does not have the right to object to their information being used for a purpose which is necessary for us to fulfil our legal obligations, including performing a contract with them (e.g. delivering their product or getting paid).

In these circumstances, Managing director, Head of Administration team or Head of Sales team could decide to refuse the request. However, it should consider whether it can 'restrict' the information so that it can *only* be used for that specific purpose (but would not, for example, be otherwise visible on the customer's account).

To help Managing director, Head of Administration team or Head of Sales team decide whether we should comply with the request, Managing director, Head of Administration team or Head of Sales team should ask the requestor to provide his/her *reasons* for the objection/erasure request (if he/she has not already done so). This allows RKG to consider whether, on balance, the request should override our interests in processing the personal data. Note that an individual does not have to provide a reason for objecting to marketing.

As a general rule, RKG should comply with all erasure and objection requests which relate to direct marketing, cookies and customer profiling, or where we have sought a specific consent which the customer has withdrawn. If we decide to comply with an erasure request, you should not delete all reference to the requestor, as RKG will need to retain a record of the request.

Data protection law also gives individuals specific rights to object to decisions being made about them which are *solely* automated, and which have a significant impact on them. An example might be a decision to hire an individual based purely on an automated process. Managing director, Head of Administration team or Head of Sales team should consider any request objecting to an automated decision, to determine whether it falls within the scope of this right.

Step 8 - Provide the response

If Managing director, Head of Administration team or Head of Sales team have decided a specific request should be refused in its entirety, Managing director, Head of Administration team or Head of Sales team should draft the response to the requestor. The response will need to set out our reasons for refusing the request. If RKG have decided to respond to an erasure request by 'restricting' the personal data, this should be explained in the response.

Where Legal have decided RKG can comply with the request, HR/Customer Services can respond to the requestor. In respect of **access requests**, there is a template response at Annex 1.

If the request is made via email, we should provide the response via email (or if the individual has requested an email response). Only if requested by the individual, Managing director,

Head of Administration team or Head of Sales team should consider whether it is possible to provide the information in a machine-readable format.

In other cases, however, we can send the response via post.

Managing director, Head of Administration team or Head of Sales team should review any response before it is sent.

Last updated: [TBC]

Annex 1: Template response to an access request

[By email or post]

Dear [Requestor]

I write in response to your request dated [insert].

I have attached a copy of the personal data which you requested. This is personal data consisting of [insert brief description of data, e.g. record of your purchase history, your employment record, correspondence with RKG etc.].

[Some personal data which you requested has not been disclosed, as RKG was entitled to withhold this information under data protection law.]

RKG processed this personal data for the purposes of [insert brief description of the purposes, e.g. to process an order, deal with a complaint, manage the employment relationship, conduct a disciplinary process, send you marketing].

[Insert details of third parties who have received the data: This personal data has been shared with our service providers so that they can provide services to us. It has also been shared with [insert any other third parties].]

[If the data was not obtained from the individual but from a third party, you should state the source of the data].

RKG will retain this data for [x years or until x years after our relationship with you has ended, or similar information about how the retention period will be determined].

You are entitled, in some circumstances, to request that RKG rectify inaccurate personal data, erase or restrict your personal data, or to object to RKG processing your personal data for certain purposes. However we are not obligated to comply with this request where we have a lawful basis for refusing it.

If you believe we have not satisfactorily complied with our request, please contact us. You are also entitled to make a complaint to the Data Protection Officer of Hessen, Germany.

[Sign-off]