1. Personal Data Breaches Guidelines

1.1 What is a personal data breach?

A “personal data breach” means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Accordingly, we should make sure that every kind of incident is noted and reported, such as loss of devices (laptops, smartphones), any intrusion or hacking of our websites and systems, strangers coming into our offices without supervision, incidental sending of emails to the wrong addressees, which includes personal data.

1.2 What are our obligations in case of a personal data breach?

RKG must promptly (i.e. **within 72 hours!**) notify the responsible Data Protection Authority of any breach of security measures that can reasonably be expected to pose a risk to the rights and freedoms of natural persons and the data subjects in case of a respective high risk. Furthermore, RKG might need to notify the data subjects.

*Accordingly, each RKG employee getting knowledge of personal data breaches must **immediately** report such breach to the Managing Director of RKG, irrespective of the cause and severity of such breach in order to allow them to decide whether these legal obligations do apply and to mitigate any breaches. It is very important that you make such report immediately to allow RKG to keep the deadlines.*

1.3 What needs to be notified to the data protection authorities?

Please see the attached notification form.

1.4 What needs to be notified to the data subjects?

It is important to understand that not every breach must also be notified to the affected data subjects (while the data protection authority always needs to be notified in case of a risk).

First of all, the obligation to notify individuals only applies in case of high risks for those persons. Furthermore, there are several exemptions from the notifying obligation, in particular i.e. if the data was secured, e.g. by encryption, effective mitigation measures were taken so that the likelihood of substantial consequences is mitigated or if the notification of individual persons would be disproportionate (however, in that case, a public communication would be required).

The type of information to be given is basically the same as in the attached notification form. However, a more basic, but clear and concise language is required. Please always imagine that a normal person or user without detailed IT background needs to be able to understand this notification.

Data Breach Form	Article 33 - Form for reporting incident				
Company (Controller)		*Site / Dept.*			
Email		*Other contact data*			
Today's Date		*Date & Time of Incident*		*Risk Level*	
Responsible Person (with contact information)				*No.:*	

Description of the Incident (including type of breach, affected data categories and amount of data, type and number of affected data subjects, likely impact and consequences of the breach)

Description of measures taken and Mitigation Plan

Form sent to Authority: Y/N	*Reviewed and Approved by*		*Date:*	