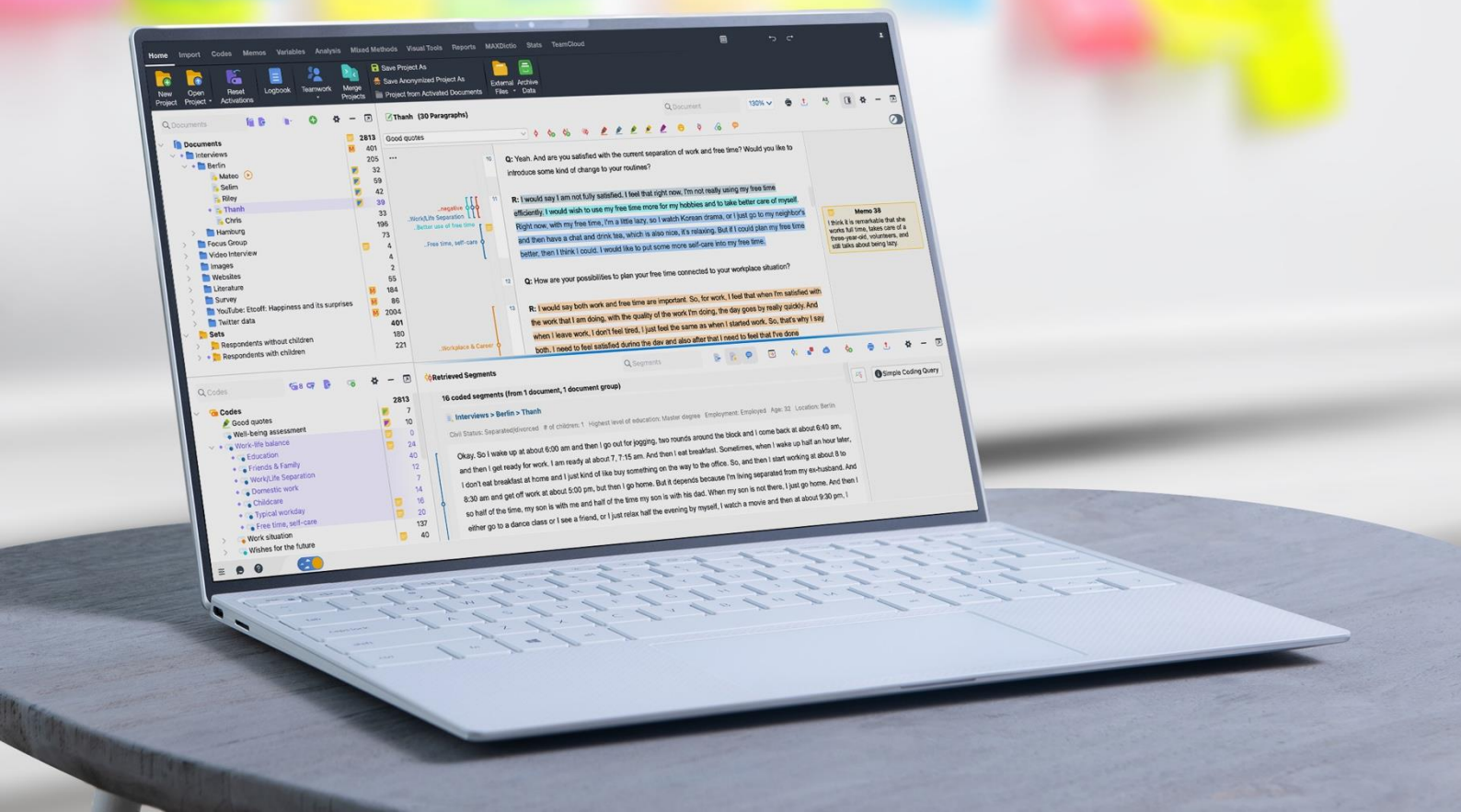
MAXQDA

Data Protection Incident Management Guidelines



In compliance with the General Data Protection Regulation (GDPR), we have established a robust data breach response plan that includes the following key notification procedures:

1. Immediate assessment: Upon discovery of a potential data breach, we immediately conduct an assessment to determine the nature and scope of the breach. This helps us understand the type of data involved and the potential impact on affected customers/users.

2. Notification to authorities: In line with GDPR requirements, if the breach poses a risk to the rights and freedoms of customers/users we notify the relevant data protection authority within 72 hours of becoming aware of the breach. This notification will include all relevant details of the breach, such as the categories and approximate number of customers/users affected, and the categories and approximate number of personal data records involved.

3. Notification to affected customers/users: If the data breach is likely to result in a high risk to the rights and freedoms of customers/users, we will promptly communicate the breach directly to the customers/users affected. This communication will be clear and transparent, explaining the nature of the breach, the likely consequences, and the steps we are taking to address it.

4. Ongoing support and information: We provide a point of contact for customers/users to obtain further information and guidance on protective measures they can take. This may include advice on changing passwords, monitoring accounts or accessing credit monitoring services.

5. Ongoing monitoring and updates: After the initial notification, we continue to monitor the situation and provide updates to both authorities and affected individuals as new information becomes available or as the situation evolves.

6. Documentation and record keeping: All data breaches, regardless of size and impact, are documented. This helps us not only to comply with the GDPR, but also to evaluate and improve our data security measures

7. Help through Cyber Risk Insurance: We are supported by IT crisis experts and data protection lawyers in the event of an incident.