University of Basel

Data Protection
Audio Transcript

Responsibility and liability

IV Interviewer
DK Danielle Kaufmann
BR Beat Rudin

[IV]: Danielle Kaufmann, Beat Rudin, a warm welcome. Today, we would like to discuss responsibility in data protection. Where does responsibility under data protection law lie and what is the meaning of legal responsibility?

[DK]: The applicable data protection law defines the responsibility. The Information and Data Protection Act of Basel-Stadt, IDG, which always applies whenever employees of a public authority or a public institution of the Canton of Basel-Stadt process personal data, states that the public institution which processes personal data in order to fulfil its statutory role – or entrusts a third party with processing the data – bears responsibility for the associated data protection.

[BR]: Of course, a public institution cannot bear responsibility – only people can bear responsibility. If the public institution is responsible, this responsibility ultimately falls upon the management: the person who holds the executive role in the public institution or the executive board.

[IV]: So that means that the head of a public institution is responsible for its data protection?

[BR]: The head of the social welfare office, the executive board of the University Hospital, or the president of the university are not responsible for every individual act of personal data processing – but they bear overall responsibility. They must ensure that responsibility is properly allocated within their organization, that it is assigned appropriately and that there is no data processing taking place in their area for which no one has been assigned responsibility.

[IV]: What does “responsible” actually mean?

[BR]: Responsible means that it must be ensured that all the requirements for the processing of personal data are upheld. This means that:

- data is only processed as stipulated by law;
- data processing is done proportionate, which means especially that only the data appropriate to, and required for, a particular purpose – to fulfill the task at hand – is processed;
- additionally, it must be ensured that data is only processed for the purpose for which it was collected;
- and finally, that the data is processed securely, which means that it is protected from unauthorized access or alteration and unintended loss.

IV: What about data storage?

[DK]: That’s an important point: the person who is responsible must also ensure:

- that the data is not kept longer than necessary to fulfill the relevant task (or than required by law);
- that the data is ultimately destroyed, if it doesn't have to be delivered to the state archive;
- that the rights of the affected individuals are guaranteed, e.g. the access to one's own personal data or the right to correct any inaccurate personal data.
- Finally, the head of the public institution is also ultimately responsible for ensuring that, in the case of outsourcing, the commissioned third party is contractually obligated to process the data exclusively in the same way that the commissioning public institution would be permitted to do. The commissioning institution remains responsible to the individuals whose personal data is being processed.

[IV]: So those who are ultimately responsible have to organize the responsibility. They do this by ensuring an appropriate organizational system, providing the necessary infrastructure for the fulfilment of the task, selecting the right staff and train them appropriately, enacting the necessary regulations and directives, and overseeing compliance with the rules. What about the staff? What do they need to do to prevent any violations of data protection?

[DK]: They process the personal data in accordance with their list of duties or assignment. They stick to the regulations and instructions provided by their employer, who bears ultimate responsibility. They ask if they don't know what they need to do to process the data in compliance with data protection regulations. And they notify their supervisor if they sense that data processing is not data protection-compliant, that regulations or instructions are incorrect, or that security of the infrastructure isn't guaranteed.

[BR]: The canton or the public institution are liable if personal rights are violated as a result of unlawful, disproportionate or insecure data processing. This can come back to fall upon staff who acted improperly. Disciplinary measures may possibly also be taken if staff violate data protection regulations.

[IV]: For the affected individuals: what can they do if they want to know whether and how their data is being processed, or if they believe their personal data is not being processed in compliance with data protection regulations?

[DK]: They have certain claims against the public institution:
- they can demand information about whether and, if so, what data is being processed.
- They can demand that inaccurate data be corrected.
- They can also demand that unlawful processing of their data be stopped.

[BR]: They can also demand that the results of unlawful processing of their data be eliminated, for example that data be deleted or that a recipient of such data be informed of its unlawful status.
They can demand an inquiry into whether processing of data concerning them was unlawful.
And, finally, where applicable, they can demand damages caused to them by the processing of their data, for example if data was released unlawfully.

[IV]: Danielle Kaufmann, Beat Rudin, thank you very much for this interesting conversation.