FIRMENVERTRAULICH

JACOBS UNIVERSITY

Jacobs University
25. May 2018

Confidentiality Obligation & Data Protection Fact Sheet

☑ Mr./Ms. (Last name and first name):

CHOWDHURY, PRIONTU

Role at Jacobs University:

Student

is hereby obliged to observe confidentiality.

In accordance with data protection regulations, in particular EU Regulation 2016/679 on the protection of individuals with regard to the processing of personal data (General Data Protection Regulation) and national data protection regulations, personal data must be processed in such a way that the confidentiality and integrity of the data is guaranteed. As part of your professional activities, you may therefore never process personal data without authorization or unlawfully or intentionally or unintentionally violate the security of the processing in a manner that leads to the destruction, loss, alteration, unauthorized disclosure of or unauthorized access to the data. You must therefore take the necessary care to protect personal data within the scope of the task assigned to you; any defects found must be reported to the line manager or the responsible body.

A leaflet with more detailed information on data protection and further information is attached to this declaration.

Violations of data protection may be punished by means of financial penalties, fines or imprisonment. Violations of data protection may also trigger a compensation claim from affected parties. A violation of data protection also constitutes a breach of employment contract obligations and may result in employment law measures.

Please confirm by means of your signature that you have read this declaration as well as the enclosed fact sheet and have taken note of your obligation to confidentiality and compliance with data protection in the company. This obligation will also continue to apply on termination of your employment with the company.

06.09.2021

Date, signature

Data Protection Fact Sheet

This fact sheet explains the main principles of data protection, informs you about your rights and supports you in complying with data protection and confidentiality.

1. What is the purpose of data protection?

Data protection is a basic right. It protects citizens against their personal rights being violated. In principle, everyone has the right to decide for themselves on the collection and processing of their data.

Data protection regulations, in particular EU Regulation 2016/679 on the protection of individuals with regard to the processing of personal data (General Data Protection Regulation, GDPR) and national data protection regulations prohibit the unauthorized collection, processing and use of personal data. However, laws may also permit the handling of personal data.

What is meant by personal data is defined in Art. 4 No. 1 of the GDPR. It includes names, contact details, banking details or information about a person's health status. Data on legal persons (e.g. company addresses) are not subject to data protection – however, other confidentiality obligations apply here, e.g. from the German Civil Code, the German Industry Regulation Code, competition and criminal law, as well as employment contract regulations on business secrecy.

2. When may personal data be processed?

Pursuant to Art. 5 (1) letter a of the GDPR, personal data must be processed in a lawful manner, in good faith and in a manner that is comprehensible to the data subject. Pursuant to Art. 5 (1) letter f of the GDPR, personal data must also be processed in such a way as to ensure adequate security of the personal data, including protection against unauthorized or unlawful processing and against unintentional loss, unintentional destruction or unintentional damage through appropriate technical and organizational measures ("integrity and confidentiality").

Pursuant to Art. 6 of the GDPR, personal data may only be processed if it is based on consent, for the performance of a contract, for the fulfillment of a legal obligation in order to protect vital interests, for a task in the public interest or in the exercise of the transferred public authority, or if the processing is necessary to protect legitimate interests after having considered the matter.

This is usually the case if you process the data to perform the tasks assigned to you, such as personnel data in the HR department or customer data as part of customer service. Permission is also deemed to exist if the data subject has given voluntary, effective and verifiable consent for the specific data processing.

Any unauthorized processing or use for other purposes is prohibited.

If you are unsure whether a specific data processing procedure is permissible, contact your supervisor or Data Protection Officer (contact details at the end of the fact sheet). This obligation continues after the end of the activity; i.e., even if you have left our company, you are still obliged to maintain secrecy about the processed data.

3. What rights do data subjects have?

Data subjects (e.g. customers or employees) have the right to information about their stored personal data. In certain cases, you may also request the correction, deletion, restricted processing, objection to or transfer of your data. Corrections may be considered if the data is incorrect. Data must be deleted if the legal reason for the collection or storage does not (no longer) exist(s) and there is no legal obligation to retain the data.

The prerequisite for this is that the data subject knows where, which and for what purpose the data is stored and used. For this reason, the data subject must be informed in detail of the data processing by the responsible body (the company) the first time their data is stored. The data protection rights of data subjects are diverse and must be complied with within one month of receipt of the application at the latest. If you have any questions regarding data protection, please contact the Data Protection Officer. However, data subjects also have the opportunity to contact the data protection supervisory authorities of the federal states.

You are not only obliged to protect the rights of others, but can also invoke these rights yourselves as employees.

4. Sanctions in the event of data protection violations

Violations of data protection may be punished by means of very high financial penalties, fines or imprisonment. For example, Art. 83 of the General Data Protection Ordinance provides for sanctions of up to €20 million or up to 4% of annual turnover for certain violations. Data protection supervisory authorities may also impose fines on employees of a company in cases of data protection violations.

A violation of data protection by employees is in most cases a violation of employment contract obligations and can result in employment law measures - from a warning to dismissal. In the case of intent and gross negligence, recourse is also possible. Criminal liability may also be considered under the provisions of the German Criminal Code (StGB) or Section 17 of the German Unfair Competition Act (UWG).

Please therefore handle personal data with care.

5. How to handle data protection correctly

Here we have put together some tips for you on what to do when it comes to data protection:

Lock confidential documents away

Are you leaving the office for a short time, going on a break or leaving at the end of the day? Do not leave confidential documents with personal data on your desk, but make sure they are securely locked away.

Do not leave windows and doors open when the room is unattended.

Dispose of documents securely

Time and again stories of company documents falling into the wrong hands by being fished out from garbage bins or wastebaskets by strangers make the rounds. Therefore, dispose of documents with personal data that are no longer required only via the special collection bins, or shred the data.

DON'T STARVE THE SHREDDER

Do not leave data on or in the copier

Collect printouts from the copier immediately.

Do not allow unauthorized viewing of the screen:

If possible, set up your screen in such a way that unauthorized persons cannot see it. Make it a habit to lock your screen manually (using Ctrl/Alt/Del +"Lock") when you leave your workstation.

WHO'S HAVING A GOOD LOOK? Change the perspective!

Use secure passwords

Examples of weak passwords are:

Have you got your password?

Never give your passwords to unauthorized persons. Never write down passwords. A common mistake is to keep a password note under the keyboard or on the screen.

Select passwords that are as complex as possible. Generally, passwords with at least eight characters consisting of upper and lower case letters, numbers and special characters are secure. Never choose trivial passwords or your name.

Supervise strangers

Talk to strangers in the building about their visit and accompany them to the employee they wish to see. Never leave cleaners or craftsmen unattended when they are in areas where personal data is processed (offices, IT rooms).

Protect confidential calls

Do you have something confidential to discuss? Then go to an area where other people cannot listen in on the call.

Requests for personal data? Check first!

Is someone requesting personal data by telephone or in person? Then make sure that the inquirer is serious, e.g. by calling back under the number given or ask for the file number or a customer number. Please refer to the company's data protection policy. Do not disclose confidential information or sensitive personal data orally. Answer any such questions in writing and, if necessary, only after consulting your superiors.

Check emails, protect recipients

Do not open emails of unknown origin or with "suspicious" attachments. If you send an e-mail to several people who are not supposed to know the addresses of the intended recipients, then set the recipients to "bcc" (= blind carbon copy; recipients' addresses are not revealed), especially when sending newsletters.

HOLLOW ... but ingenious

Restraint in the private sphere

Never disclose business information about people in private conversations or on privately used social media.

PSST … don't broadcast everything.

6. Data Protection Officer contact details

For further information and in cases of doubt, please contact your Data Protection Officer.

CONTACT DETAILS
Dr. Uwe Schläger Company Data Protection Officer Contact person: Dr. Sebastian Tausch (Legal Adviser) Konsul-Smidt-Strasse 88 28217 Bremen +49 (0)421 6966 3230 stausch@datenschutz-nord.de