[*June 12th, 2018*]

Privacy Requirements

Employee Privacy Notice T-Mobile (*Medewerker privacyverklaring*)

T-Mobile Netherlands B.V., T-Mobile Thuis B.V. en T-Mobile Finance B.V.

Version: 1.0
Date: June 12th, 2018
Status: FINAL

[*June 12th, 2018*]

Privacy Statement - Information regarding the Processing of Employee Data within T-Mobile Holding B.V.

Introduction

T-Mobile Holding B.V. is referred to in this notice as "**T-Mobile**", "**us**" or "**we**". T-Mobile needs to collect and process certain information about individuals in order to run its business. This information relates to, amongst others, current, past and prospective employees, workers, job applicants, customer, suppliers and other individuals T-Mobile does business with.

We are responsible to the individuals of whom we collect and process data to ensure that we use their information with care and in compliance with privacy and data protection laws (**GDPR**). Our brand and organisational values require good data governance procedures, including those which are explained in this Privacy Statement ("**Statement**").

This Statement is intended to give you an overview of how T-Mobile processes your personal data within the framework of your (employment) relationship and your rights under data protection law.

TABLE OF CONTENT

A. WHAT CAN YOU EXPECT FROM T-MOBILE

1. Who is responsible for your data processing and whom can you contact?

We are the responsible data controller. If you have any questions or comments regarding the processing of your data, please contact HR Service Desk by calling 06-14092124.

2. What personal data do we process?

We collect and use information that concerns you in connection with your employment at T-Mobile. Relevant personal data we process are, in particular:

- Personal details (name, date of birth, address, and other contact details)
- Nationality/citizenship and, where applicable, residence permit and work permit
- Certificates, professional appraisals, and proof of qualifications
- Health and benefit related information
- Information about your family (e.g. partner & children) and marital status
- Information about use of T-Mobile systems
- Your bank details
- Tax, insurance, pension data
- Photos and camera footage
- Information regarding previous employment and sideline employment
- Information regarding your employment relationship (job description, organizational unit, professional contact details, personnel number, time recording, etc.)

3. Why do we process your data (purpose of the processing) and on what legal basis?

Please find below an overview of all purposes of processing of your data and the legal ground which underpins this use. Below the tables you can find an explanation of the legal grounds.

a) To set up your labour agreement

Goal	What data is processed	Reason	Retention Period
Setting up your labour agreement	All personal data in contract or delivered by entering the contract	Execution of labour agreement	Maximum of 7 years
Execution of labour agreement (i.e. payment of salary)	All personal data in contract or delivered by entering the contract	Execution of labour agreement	Maximum of 7 years

b) To create a personnel file

Goal	What data is processed	Reason	Retention Period
Setting up your employee file to keep track of performances, coaching and personal development	Appraisal interviews, certificates, performance management	Legitimate business purpose	Maximum of 2 years after end of contract
We register your absence, sickness, leaves (pregnancy, parental, care or adoption) and your reintegration file to ensure you receive the help and benefit you are entitled to.	Name, address, e-mail, city, country of residence, phone number, gender, start and end date of leave or sickness, sofi number, name of child, gender of child, date of birth child, reason sickness leave	Legal obligation	Maximum of 2 years after end of contract
We need to register all personal administration, payroll, salary payments, etc.	Name, address, city, marital status, business email, phone number, salary slips, labour agreement, benefits, pension, bonus, bank account	Legal obligation	Maximum of 7 years after end of contract
We process your information to end your labour agreement and (when applicable) to make sure you receive your pension benefits.	Name, business e-mail, phone number, date of birth, employee code, contract ID	Execution of abour agreement	Maximum of 7 years after end of contract

c) Provide all the facilities for you to be able to work

Goal	What data is processed	Reason	Retention Period
To make sure you can use our follow-you printing system, access the building, get new software, etc. we need your personal data.	Name, business e-mail, employee code, photo	Legitimate business purpose	Maximum of 2 years after end of contract.
In order to provide you a laptop, parking transponder, locker, etc. we need to process some personal data	Name, address, business e-mail, employee code, date of birth, phone number, transponder number, licence plate, signature	Execution of labour agreement	Maximum of 2 years after end of contract

d) To create a safe and healthy work environment

Goal	What data is processed	Reason	Retention Period
A safe and healthy workplace	Camera footage	Execution of contract	Maximum of 4 weeks
Determine your identity and preventing identity theft	A copy of your passport	Legal obligation	Maximum of 5 years after end of contract
When we suspect a case of fraud (and only then) we will read your business e-mail. Permission for the CSO and HR director is requested before we are able to read these emails.	Name, address, business e-mail, employee code	Execution of contract	4 weeks after closing case

e) Recruiting and selecting new personnel

Goal	What data is processed	Reason	Retention Period
Recruitment and selection of new candidates	Name, address, e-mail, date of birth, certificate of conduct, resume, motivation letter, references, notes, assessment reports	Legitimate business purpose	Maximum of 4 weeks unless permission is given to keep for 1 year

Making sure you meet all the requirements for the position. In order to do so we conduct a credit check and ask for a certificate of conduct	Credit check and certificate of conduct	Legal obligation	Maximum of 4 weeks after the receiving the certificate

f) To create a T-Mobile Community

Goal	What data is processed	Reason	Retention Period
We use Workplace to build a T-Mobile community. At Workplace everyone can share what he/she is working on. This way we keep each other up to date on everything that is happening in T-Mobile.	Photos and films	Execution of contract	Maximum of 2 years after end of contract

g) To be create a good employer-employee relationship

Goal	What data is processed	Reason	Retention Period
In order to provide you a gift for a newborn we process data of your children. We can only do so if you register this information	Name of child, gender, date of birth	Execution of contract	Maximum of 2 years after end of contract

Explanation of legal grounds.

a. For the execution of the labour agreement

We process your data for employment-related purposes if necessary for the creation, execution or termination of the employment relationship or fulfillment of any rights and obligations of the employee representatives arising from a law or a collective agreement. As such, we process your data, for example, as part of HR management, administration and development as well as business communications.

b. As part of our legitimate interests (Art. 6 (1) (f) GDPR)

Where required, we also process your data in order to protect our legitimate interests and those of third parties. Examples:

- Measures for building and plant safety (e.g., access control),
- Training and development
- Reporting
- Measures for business management and risk management within the Deutsche Telekom Group (e.g., audits conducted by Group Audit)

c. On account of legal obligation (Art. 6 (1) (c) GDPR)

As an employer, we are subject to various legal obligations, for example, resulting from tax legislation (payment of income tax on wages and salaries), social security legislation (payment of health insurance contributions, etc.), Works Constitution Act (provision of data for works council elections, etc.).

d. On account of your consent (Art. 6 (1) (a) GDPR)

We may also process your data on the basis of consent, if the consent meets the legal requirements. Any consent that has been given may be withdrawn at any time with effect for the future.

4. Who has access to your data?

Within T-Mobile, the units with access to your data are those which require for the purposes of processing. As part of any processing, we may also use service providers and data processors (Art. 28 GDPR). In all cases we remain responsible for protecting your data. When working with your data, the partner must follow our instructions at all times. To ensure that this is the case, we signed a Data Processing Agreement (DPA) to make sure they follow our instructions on how to process your data and to make sure they are compliant to the GDPR.

Where applicable, we share your data with external companies, who process your data under their own responsibility. They are so-called controllers who also collect your data under their own responsibility. Data that they will not share with T-Mobile. For example a company doctor, psychologist, a reintegration specialist or an auditor.

Personal data will also be shared with government bodies, authorities and/or law enforcement officials if required for the purposes mentioned in this Notice, if mandated by law or if required for the legal protection of our legitimate interests in compliance with applicable laws.

5. Is data transferred to third countries?

In principle, your data is processed in the Netherlands and in other European countries.

If, in exceptional cases, your data is processed in countries outside of the European Union (known as "**third countries**"), this takes place only if legally required (for example, due to reporting obligations under tax law), you have expressly provided your consent, or it is required as part of the employment relationship, for example for business communications. Data processing is also permitted in a third country if the European Commission has decided that there is an adequate level of protection in a third country (Art. 45 GDPR). If the Commission has not made such a decision, we or the service provider transfers personal data to a third country only if appropriate safeguards are provided for an adequate level of protection. T-Mobile uses the standard data protection clauses (standard contractual clauses for the transfer of personal data) recognized by the European Commission as such safeguards. For the transfer of data within the Deutsche Telekom Group we use our Binding Corporate Rules Privacy. Both are available here: www.telekom.com/laws-and-corporate-rules

6. To what extent does automated decision-making take place?

To create and execute the employment relationship we do not use automated decision-making in accordance with Art. 22 of the GDPR. If we use these processes in individual cases, we will inform you separately in accordance with legal requirements.

7. What data protection rights do you have?

Internal and external employees and job applicants at T-Mobile have several rights when it comes to the use of their personal data. For example, you have the right to have access to your personal data that we collected. Furthermore, you can ask us to adjust this information or to have your data erased out of our systems. You can also object to us using your data and when you gave your consent to us to use your information, you have the right to withdraw this consent at any time.

As an external employee you also can see most of the personal data that we have by logging into YouForce and open your digital personnel file. If you want to use one of your privacy

rights, you can file a request at the HR Service Desk under the header "Privacy/GDPR/AVG" and select the right you want to obtain. Below you can find a more detailed explanation on how you can file a request.

When you are an external employee or a contractor, we collect and keep very limited personal data. We only have your name, date of birth, phone number, email address and your business email address. When you decided filled out this (and additional) information on T-Share by making an online profile for the 'Wie is Wie' page we also have this additional information. Furthermore we signed a Data Protection Agreement (DPA) with your supplier or agent to make sure you are also complaint to the GDPR.

When you are a job applicant and you did not receive a job offer, then we will keep your personal data for 4 weeks. Unless you gave us permission to keep your data, then we will keep your data for 1 year. This way we can reach out to you when we have another job offer that matches your ambitions and talents. At any time you can withdraw your consent and have us delete your personal data. You can do this by sending an e-mail to: resourcing.center@t-mobile.nl.

We will respond to any of your requests within 30 days.

1. Access

You have access to most of the personal data that we have from you. You can log into your YouForce account to open your personnel file. Are you looking for something that you cannot find in YouForce? Please file a request in the HR Service Desk (under the header Privacy/GDPR/AVG – Access) for your specific request. If you are an external employee you can ask your manager to have insight in the personal data that we have from you. For each request we will investigate whether we can meet this request.

2. Rectification

Did your personal data change, for example because you recently moved? Then you can change this by yourself in YouForce. We advise to check your personal details yearly to make sure your personal data is up-to-date. If you are an external employee, you can hand over your new details to your manager, so he or she can adjust your information. Don't forget to pass along this new information to your supplier as well!

When you are a job applicant and you want to change the personal data that we have from you, for example an updated version of your resume or a new email address, please send an email to: resourcing.center@t-mobile.nl

3. Erasure

You can ask us to erase your personal data from our systems. However, we will not be able to meet all these requests since we either have a legal obligation to keep some information or we need this information to be able to carry out our obligations as an employer. Do you still want us to erase some of your data? Please file a request at the HR Service Desk (under the header Privacy/GDPR/AVG – Erasure) for your specific request. When you are an external employee you can refer to your manager for this request. For each request we will investigate whether we are able to meet your request or not.

As a job applicant you can ask us to delete the personal data that we have from you at any time. Please do so by sending an email to: resourcing.center@t-mobile.nl. We will delete your personal data immediately.

4. Restriction

You can ask us to restrict the use of your data. For this privacy right applies as well that we will not be able to meet all the requests for the same reason as the one above. Do you still want us to restrict the use of your personal data? Please file a request in the HR Service Desk (under the header Privacy/GDPR/AVG – Restriction) for your specific request. When you are an external employee you can again ask your manager to restrict us for the use of your data. For each request we will investigate whether we can meet your request or not.

5. Data Portability

When you stop working for T-Mobile and you want to take some of your personal data to your new employer, you can do so by requesting this data within the HR Service Desk (under the header Privacy/GDPR/AVG – Data Portability) for your specific request. As an external employee you can ask your manager for the data that you would like to take to your new employer. However, please take into account that we might not have the data that you need.

6. Objection

You have the right to object to us using your personal data for reasons other than the data was collected for. Please notify us for what reason you want to object to us using your personal data and indicate to what data you are objecting. You have also the right not to be subject to a decision based solely on automated processing, including profiling. In some cases you can object to automated decision making, You can do so by filing a request in the HR Service Desk (under the header Privacy/GDPR/AVG – Objection). As an external

employee you can again notify your manager that you want to object to use of your data. Per request we will investigate whether or not we can meet this request.

Beside these 6 privacy rights you also have the right to withdraw from the consent that you have given to use your personal data. Furthermore you have the right to file a complaint regarding the processing of your data within T-Mobile. You can file these complaint at the DPO of T-Mobile or in the second instance to the "Autoriteit Persoonsgegevens'.

B. WHAT WE EXPECT FROM YOU

1. Golden TMNL Privacy Rules

While we have taken a number of steps to secure and protect personal data and other valuable information within our company, much of that protection relies on the proper handling of information by employees of T-Mobile.

In order to protect this information and to comply with data protection laws, we ask that you make yourself aware of the guidelines described below. Here are some key points to remember when you deal with personal data:

1. Ask yourself what you really need the information for. Then do not use this information for any other purposes.
2. If you have information, make sure it stays complete and up to date.
3. Do not simply share information with others.
4. If you have information, make sure that nobody can get to it and destroy that information when you no longer need it.
5. Be open and transparent to people on whom you have information: tell them what you do with their information, what you need it for, where and how long you are going to store it, etc.

Besides these "golden" TMNL privacy rules there are other points to remember:

- Think about your responsibilities under this Statement and our further data security guidelines and how they impact on your day-to-day activities.
- Double check the recipient's details before sharing data. Are you sending data to the right individual?
- Use password protection for documents and files, wherever appropriate.

- If information is available on the T-Mobile network, use links to such information instead of the actual documents when sending the information to colleagues.
- Take a common sense approach when deciding how to protect, use and delete personal data. Think about how you would like your personal information to be treated and treat others' information the same.

This section is meant to give you general guidance and is not a comprehensive or exhaustive guide. If your function requires this, for example if you work a lot with personal information and computer systems, you may have additional responsibilities and guidelines to follow. Please ask your manager.

2. Keeping data secure and data breaches

The security obligations that you have as further described in the Policies mentioned below are not just about personal data but about all information, IT and communications systems. You are responsible for the security of the equipment allocated to or used by you, and should make sure it is not used by anyone other than in accordance with the applicable policies. You can find information about your security obligations on T-Share *[https://t-share.nl/groups/161-t-mobile-security/welcome]*.

You are obliged to report an invasion of privacy. A data leak breach is an incident whereby personal data ends up with the wrong people. "Wrong" people is a broad concept in this case. They could, for example, also be colleagues who do not need this data for their work, or customers who can look over your shoulder at a screen in a shop and read data belonging to other customers.

If you suspect a data leak breach, get in touch with your manager and together take a look at the bottom of the T-Share home page to see how your report a data leak breach.

C. QUESTIONS AND REPORTING

You are encouraged to report suspected violations of this Statement to your department manager or the Data Privacy Officer (privacy@t-mobile.nl).

In case this is not an option or if you wish to report anonymously, you can report via *Tell me*. Please refer to this link for more information on the reporting procedure.

Any employee or other staff member who believes that their data protection rights have not been respected is encouraged to bring this to the attention of his or her manager

You also have the right to file a complaint with the local data protection authority (in the Netherlands this is the *Autoriteit Persoonsgegevens*) or to seek a remedy through the courts if you believe your rights have been breached.

Date of publication: 12th of June 2018