Privacy statement for non-staff members

EPZ, Borssele, the Netherlands

24 May 2018

About this privacy statement

This is the privacy statement of EPZ N.V. We explain in this statement how we guarantee privacy for persons who have or have had direct contact with us as a visitor, contractor, temporary employee or supplier. With this privacy statement, we meet the requirements that the General Data Protection Regulation stipulates for EPZ as a controller.

We may amend this privacy statement. This version was drafted on 24 May 2018. The most recent version is always available on epz.nl.

Contents

This statement contains information about the following topics:

1 What is personal data?

Personal data is information that relates to you or that we can link to you.

For secure and responsible business operations, we process your personal data[1] if you perform work for us as a contractor, temporary employee or supplier, or if you visit our sites. Here we have in mind data that you or your employer supply, such as your name, address or email address. Camera images for security purposes or that monitor employees' health because we work with radiology are also data that we could link to you.

If you are a self-employed or a one-man business, general partnership or partnership, Then you are considered to be a person and it will also concern data that relates to you directly or indirectly.

[1] 'Processing' is a legal term. It is a very broad concept. It concerns everything you can do with personal data. From collection to destruction.
The General Data Protection Regulation defines 'processing' as 'the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data.'

2 What do we use personal data for?

For your safety and security and that of others, it is important that we know who you are. That is why we ask for and process your personal data.

We may use your personal data to implement our agreements

We may use your personal data for the following purposes:

- To find out whether you can perform work for us.
- To ensure that we know who you are so that you can work with us or for us.
- To contact you.
- To enter your information in our administration properly and to update it if there are changes.

We may use your personal data in the interests of safety and security by reducing risks

We are jointly responsible for the safety and security of you, ourselves, the environment and the nuclear sector. That is why we use your personal data to reduce risks and protect our interests. You may or may not always be aware when we use it.

You will be aware when

- we carry out alcohol tests to ensure we have a safe working environment.
- we screen everyone who works with or for us, if the work requires this, or we engage a security company to carry out this screening. We want to know who you are if you perform work for us. We will always ask for your permission and cooperation for a screening.
- we ask our visitors to identify and register themselves so that we know who is at our sites.
- we check hand luggage and coats using baggage scanning equipment or manually if it is not possible to scan it.
- if you are entitled to a personal access pass, we ask you for a passport photo that we put on your pass and in our access systems to make sure that you are the only one using your pass.
- we monitor your safety using CCTV monitoring if you work in confined spaces, so that we can intervene in time if the situation is unsafe.

You will not be aware when

- we monitor your activities on our systems and networks. For the purposes of ensuring safety, we find out what is going on our systems and networks
- we monitor our grounds using camera surveillance. If there is a suspicious situation, we may review and share the images with the police.
- we record incoming and outgoing telephone calls and share them with the police if it is in the interests of EPZ's security.

We may use your personal data to comply with the law

EPZ is obliged to comply with its obligations under domestic and international legislation. To be able to fulfil these obligations, we use your personal data to:

- measure dose data when performing radiological work. We pass this dose data on to the dose registration system.
- identify you when you perform work at EPZ. We ask you to identify yourself with a valid ID and we record various details. We require additional identification for areas with a higher security interest.
- determine whether you have suitable skills and qualifications.

3 Whose personal data do we have?

We have the personal data of everyone who has or has had direct contact with us as a visitor, contractor, temporary employee or supplier.

So this includes contact persons and representatives of business clients and suppliers who visit EPZ.

4 Which personal data do we collect?

EPZ processes personal data for various purposes.

We collect information about who you are and how we can reach you

We process this information

- Your name, date of birth and the name of your company if you perform work for us.
- Your passport photo and possibly biometric features if you have a personal access pass issued by us.
- The security features of your ID document and the information on your ID document.
- Your contact details.

These are the purposes for which we process data

- If you enter the EPZ grounds, we have to determine your identity. For this purpose, we will identify you on site based on your ID and check it for authenticity by verifying the security features.
- If you perform work for EPZ, we must be able to identify you and we will do so based on a personal access pass. For this we use your identity information, including a passport photo. If you need access to areas that have extra security, we ask for additional biometric features.
- If you are going to carry out radiological activities or if EPZ hires you, EPZ is legally obliged to use your citizen service number.
- If we want to contact you, we use your contact details or we approach your employer (if applicable).

This is how long we keep your data

- Your name, date of birth, company name, contact details, passport photo and possibly biometric features are stored for a maximum of six months after the right to access our grounds expires.
- We do not store the verification of your ID security features or a copy of your ID.

We collect information about where you are and what you do

We process this information

- Video recordings of you taken with security cameras plus location and time information when you are in EPZ buildings and on EPZ sites.
- Video recordings of you taken with safety cameras when you work in confined spaces.
- Undesirable safety and security observations, such as finding undesirable and unlawful items after checking hand luggage and coats, or a positive result for an alcohol check.

These are the purposes for which we process data

- EPZ uses camera surveillance to guarantee safety and security. We use these images to monitor our grounds and our buildings. If there is an abnormal situation, we can review the images under strict conditions and we may pass them on to the police.
- For your safety, live camera surveillance takes place while you work in confined spaces. In the unlikely event that something happens during this work, we can intervene straight away.
- To guarantee safety, EPZ monitors alcohol consumption and checks whether unwanted and unlawful items are taken on to and off the premises. We report any undesirable or unlawful incidents to your employer.

This is how long we keep your data

- Images recorded using camera surveillance are stored for up to 168 hours, or after incidents we have detected and the associated sanctions have been dealt with. Images that have been passed on to the police are the responsibility of the police.
- Images used to monitor confined spaces are kept for 24 hours or until after detected incidents have been dealt with.
- We store information about undesirable or unlawful incidents for a maximum of 24 months after the right to access our grounds has expired.

We collect information about your qualifications and education

We process this information

- Your certificates for safe working practices obtained via our electronic learning environment.
- Your qualifications, for instance, medical examination certificates (suitable/not suitable), vocational education diplomas and SCC certificates.
- Your access documents, for instance, certificate of conduct, certificate of no objection and/or a statement of confidentiality.

These are the purposes for which we process data

- We work safely or we don't work at all. To be able to work safely, we want to be sure that we work with qualified people. For this we require proof of your qualifications and training.
- Your access document is used as a security tool to deter unwanted persons from entering our premises, and to guarantee the non-disclosure of confidential information.

This is how long we keep your data

- We keep a copy of your certificates, qualifications and access documents for a maximum of 24 months after the right to access our grounds has expired.

We collect information about your use of our systems and networks

If you use our systems or networks, we record certain information.

We process this information

- Your IP address: the address of your computer or mobile that is needed to ensure that computers can communicate with each other.
- Information about the use of our applications and systems: we record your actions when you log on to our systems and applications.
- Information about the use of the internet and websites accessed from our systems and networks: when you use our systems or networks to access the internet and websites, we check which websites you visit.

These are the purposes for which we process data

- We keep IP addresses to prevent abnormal situations.
- We keep records of the use of our applications and systems to detect misuse of these applications and systems.
- We use data about the use of internet and websites to counteract malicious software from suspicious websites. In addition, we restrict access to websites and services that are a heavy burden for our systems and networks, such as streaming of online radio and video content.

This is how long we keep your data

- We use information about the use of our systems and networks for three months at most.

We collect sensitive information

Processing sensitive personal data is subject to stringent rules.

We process this information

If you require access to extra secure areas, we process the following sensitive data:

- Biometric information (palm scans).

If you perform radiological work for us, we process the following sensitive data:

- Citizen service number.
- Dose data.
- Medical suitability certificate.

If you perform work for us as hired staff, we process the following sensitive data:

- Citizen service number.

These are the purposes for which we process data

- Your palm scan is used as an additional security tool.
- We are required by law to measure your exposure to radioactivity if you perform radiological work for us. This dose data says something about your health, for example, if you have recently been exposed to radioactivity for medical reasons.
- We are required by law to record your dose data in a dose registration system. An institution has been designated by law to manage this system and this institution uses citizen service numbers. We need your citizen service number to record your dose data in this system.
- Pursuant to the 'Mandatory Use of Citizen Service Numbers Implementation Regulations', we are obliged to use citizen service numbers when hiring employees.
- The law sets requirements for the medical suitability of persons performing radiological work. We ask you for a certificate that we register in our administration.

This is how long we keep your data

- Your biometric data will only be stored in an irreversible encrypted form without the intervention of persons or other systems. We keep your encrypted information for a maximum of six months after the right to access our grounds expires.
- We are legally obliged to store your dose data including your identification information until your 75th birthday, but for at least 30 years after you perform work at EPZ.
- We comply with tax legislation by storing your data for the purpose of hiring you; the retention period for this information is seven years.

5 With whom do we share personal data?

In principle, we do not share your information with anyone. We only do so if there is a good reason or if we are obliged to do so. For instance, if you commit a crime, we may report it. In some cases, we share your data with another party or organisation on the basis of an agreement or regulation.

There are stringent regulations for sharing personal data. It goes without saying that we comply with these regulations. We only share the personal data that is required to provide a good service and we reach proper agreements with those service providers about what they are permitted to do with that personal data. We lay down these agreements in contracts.

We reach agreements with our service providers about:

- Confidentiality
- Who gets access to the data (logging)
- Which data people may access and process
- Encryption of our data during transmission and when it is stored
- Appropriate technological and organisational protection measures
- Recording incidents and access to the data
- Reporting and monitoring of incidents and data breaches
- Audits

We share your personal data with the Nuclear Research and Consultancy Group (NRG)

If you perform radiological work for us, we are legally obliged to measure your exposure to radioactivity and to record this dose data in a dose registration system. We pass your dose data on to the NRG, which processes the dose data in the National Dose Registration and Information System (NDRIS).

We share your personal data with the IT system and network manager

We use a service provider who designs, manages and improves our systems, networks and applications for us. In some cases, this service provider may gain access to the following personal data:

- Information about who you are, i.e. your name, date of birth, company name, contact details, passport photo.
- Information about your qualifications and education, i.e. certificates, qualifications and access documents.
- Information about your use of our systems and networks, i.e. logging data about systems and applications, website internet traffic, IP addresses of systems that log on to our networks.

We share your personal data with the Security Department

We use a service provider who designs, manages and improves our monitoring systems, networks and applications for us. In some cases, this service provider may gain access to the following personal data:

- Information about where you are and what you are doing, i.e. video recordings taken with security cameras plus location and time information, records of the use of access passes.

We share your personal data with the CCTV surveillance supervisor

We use a service provider who provides a CCTV monitoring system for the remote monitoring of work performed in confined spaces. This system processes the following personal data:

- Information about where you are and what you are doing, i.e. video recordings taken with safety cameras.

We share your personal data in an online learning environment

We use a service provider that provides an online learning environment for offering courses that are required before you can perform work at EPZ. This learning environment processes the following personal data:

- Information about who you are, i.e. your name, date of birth, contact details, company name.
- Information about your qualifications and education, i.e. exam results and certificates for courses taken in this environment.

6 This is how we look after your personal data

We spend a lot of time and money on the security of our systems and personal data.
We have an organisation that monitors how personal data is used and protected.

All our employees have signed a statement of confidentiality. We handle information that you entrust to us with due care; only authorised personnel may access and process your data.

We have liaised with the EPZ Works Council about the storage of data, including this document.
The following authorities supervise us:

- The Dutch Data Protection Authority. This authority monitors whether we comply with the General Data Protection Regulation.
- The Authority for Nuclear Safety and Radiation Protection. This authority supervises the nuclear sector in general, and so it monitors us too.

7 Checking or changing your personal data

You are entitled to inspect your data that we have recorded. If, in your opinion, the information is incorrect or you wish to object to the processing, you can have it rectified, limited or deleted.

You can exercise these rights by submitting a **written request** to the Privacy contact person. Please provide a description of your request, the data it concerns and your relationship with EPZ. EPZ will first establish the validity of the request by verifying the identity of the applicant, by telephone, email and/or via the registration system of EPZ. If the application is valid and well founded, EPZ will process the request and inform the applicant in writing within four weeks of receiving the request. If the application is not valid and not well founded, EPZ will reject the request within four weeks and inform the applicant about the reason for the rejection.

EPZ will ensure that the actions prompted by the decision to improve, supplement, delete and/or block the data are carried out as soon as possible. If improvements, additions, deletions and/or protection of data takes place, EPZ informs third parties about this if third-party rights are also at stake, and we ensure that the third parties amend their data accordingly. EPZ informs the person making the request about the third parties that it has disclosed information to.
If EPZ rejects the request or if no agreement is reached about the request, the applicant has the option of contacting the Dutch Data Protection Authority.

8 Contacting us

For any questions you may have about your privacy at EPZ or for submitting written requests, you can contact our Privacy contact person:

N.V. EPZ
Attn S. d'Hooghe (Privacy contact person)
PO Box 130, 4380 AC Vlissingen | Zeedijk 32, 4454 PM Borssele, The Netherlands
Email: incident@epz.nl
Telephone: +31 (0)113 356 518