# 1 DATA CENTER VISIT

We (Interconnect Services B.V.) process your personal data if you visit one of our data center locations. In this privacy statement we give you more information about processing your personal data.

# 2 FREQUENTLY ASKED QUESTIONS

Which personal data is processed?

In the table below you can see which personal data we process per processing activity.

| Processing activity | Personal data |
|---|---|
| Authentication, authorization verification and visit registration. | *Visit registration*<br>• First name(s)<br>• Initials<br>• Last name<br>• Company/organization<br>• Access rights (racks/spaces)<br>• To visit (racks/spaces)<br>• Planned visit time<br>• Check-in and check-out time<br>*Document information*<br>• Offered ID document type (passport, driver's license, residence permit document or ID card)<br>• Last 4 characters of the document number<br>• The "valid to" date of the document<br>• Scan result (approved, not approved)<br>• Scanned first name(s), initials and last name<br>• Passport photograph |
| Registration for the biometric access control and its use.* | *Biometric registration*<br>• First name(s)<br>• Initials<br>• Last name<br>• Fingerprint template (landmarks/minutiae)<br>• Access rights (corridor) doors<br>*Biometric access logs*<br>• Opened (corridor) doors<br>• Date/time opened (corridor) doors |
| Camera security | *Camera images*<br>• Camera images (inside and outside) |
| Reporting about data center visits to the customer. | *SLA reports*<br>• Everything under "*Visit registration*" (excl. access rights)<br>• Everything under "*Biometric access logs*" |

** This does not apply to guest visitors who visit the data center under the supervision of an authorized contact.*

Please note: We do not store a copy of the ID document. The passport photograph, first name(s), initials and last name on the ID document are visible for the DC Host/Receptionist for verification for a short period. These are not stored (we store the name that is registered in MyInterconnect). The employee has no access to the entire document. In addition, no complete scans of the fingerprint are stored, but only landmarks (so-called "minutiae"). The privacy of the visitor is thus breached as little as possible.

### What is the purpose and basis of processing?

With the exception of the "SLA reports" processing, the purpose of the aforementioned processing is to secure our data center locations against unauthorized access. In addition, the registration data gives us insight into the number of visitors present in the building, which is important in the event of a calamity, for example.

We process the personal data based on a legitimate interest, namely the security of our information systems and that of our customers. A high level of security is necessary to reduce the identified information security risks and to comply with contractual obligations as well as laws and regulations.
The prohibition on processing biometric data does not apply because processing is necessary for authentication and security purposes (see also Art. 29 of the Dutch GDPR Implementation Act). Interconnect has set up the biometric access control in such a way that the impact on the privacy of the person concerned is minimal and is in proportion to the purpose.

The SLA reports are produced to inform the customer about the use of the purchased service(s), compliance with the agreed service levels and to enable them to review (physical) access logs.

### Can I gain access to the data center locations without providing personal data?

The aforementioned processing activities are necessary to maintain the required security level. It is therefore not possible to access our data center locations without providing the aforementioned personal data. If you do not want to provide your personal data, please contact your employer/client.

### Where is my personal data stored and how is it secured?

Your personal data is stored in our own data centers and on our own systems. Your name, company details and access rights (see: "*Visit registration*") are also stored in a Cloud CRM application hosted by our supplier within the EU. Only Interconnect employees who need access as part of their job duties gain access to the personal data.

We take appropriate organizational, technical and physical security measures to prevent unauthorized access and abuse of systems and personal data. These measures are monitored and periodic checks take place to test the effectiveness of the measures. In addition, we have the following certifications regarding information security:

- ISO 27001
- PCI-DSS Level 1 Compliance
- SOC2 Type 2 (ISAE3000)

### How long will my personal data be stored?

We maintain the following retention periods:

| Personal data | Retention period |
|---|---|
| Visit registration | 12 months |
| Document information | 12 months |
| Biometric registration | As long as the person concerned is still a contact person with DC visit rights for at least one customer and has visited the data center in the past 6 months. |
| Biometric access logs | 12 months |
| Camera images | 4 weeks |
| SLA reports | Up to 12 months after termination of the agreement |

### Is my personal data provided to other parties?

Some other parties receive your personal data. For example, we use a Cloud CRM application that is hosted by our supplier within the EU. Only your name, company details and access rights (see: "*Visit registration*") are provided. In addition, our customers have the opportunity to receive reports on data center visits to their space. If this report is provided to them, the information as described in "SLA reports" will be shared. We do not share your personal data with other parties, unless we are legally obliged to do so.

PLEASE NOTE: If you try to open a (corridor) door for which you do not have access rights, this will be represented anonymously in the reports for the customer in question. In this case your name and company name will not be provided to another customer.

### What are my privacy rights?

You have the right to request access, rectification (correction), erasure (removal) and restriction of processing. In addition, you have the right, for reasons relating to your specific situation, to object to the processing of your personal data. We will cease processing unless we can demonstrate there are compelling, legitimate grounds for processing which override your interests, rights and freedoms or unless processing is necessary for the establishment, exercise or defence of legal claims.

Exercising the right to erasure, objection and restriction of the processing may limit your ability to visit our data centers. You can submit your request to the Risk & Compliance team and we will respond in writing within one month.

### I have a complaint

You can submit a complaint to us if you are not satisfied. This is possible via the contact details at the bottom of this privacy statement. We will handle this complaint and get in touch with you as soon as possible. You have the right to submit a complaint to the Dutch Data Protection Authority (Dutch DPA) if you believe that we do not help you or do not help you sufficiently or act in violation of the General Data Protection Regulation (GDPR). You can submit this complaint to the Dutch DPA via the website: https://www.autoriteitpersoonsgegevens.nl/.

# 3 CONTACT INFORMATION

You can contact us to submit a request or ask questions about processing personal data.

Interconnect Services B.V.
Het Sterrenbeeld 55
5215 MK 's-Hertogenbosch, the Netherlands
riskcompliance@interconnect.nl
+31(0)73-8800000