

PRIVACY NOTICE

Digital Realty Trust Inc. and its affiliated entities (collectively, “Digital Realty”, including but not limited to the Interxion EMEA Group and may also include the terms “we”, “us”, “our” or similar terms) are committed to respecting and protecting the privacy rights of individuals who interact with us through our websites and our portals, when accessing our premises, when using our products and services, or with whom we otherwise communicate.

(A) This Privacy Notice

This Notice describes how Digital Realty collects, uses, shares and/or otherwise processes your personal information in compliance with all applicable data protections laws in the countries and regions in which we operate and in the context of our business activities. It is addressed to all individuals outside our organization with whom we interact (together, “you”). Defined terms used in this Notice are explained in this Notice or in Section (O) below.

When using the term “Personal Data” we mean information that relates to you as an individual and that allows us to identify you either directly or in combination with other information that we may hold.

This Notice may be amended or updated from time to time to reflect changes in our practices with respect to the Processing of Personal Data, or changes in applicable law. We will notify you in case of material changes. We encourage you to read this Notice carefully. If you have any questions regarding how Digital Realty processes your data, please contact the Digital Realty Privacy Team. For relevant contact details please see section (N).

(B) Your relationship with us

In the context of our services, we may collect or obtain Personal Data about you as an individual in the following situations:

- As a visitor to our office locations and/or data center facilities
- When you use and/or interact with us through our websites or through social media
- In the context of our business relationship (including, though not limited to customer, supplier, service provider)
- As a registered customer representative using and accessing our Portals
- As an authorized representative of our customers, suppliers or service provider(s) accessing our secure data center facilities
- As an applicant in our recruitment process
- As a business representative who corresponds with us via email, voicemail or audio or video conferencing

- As a business prospect representative who shows interest in our services
- As a participant of our conferences, events and learning sessions

(C) Collection of Personal Data

We may collect or obtain Personal Data from you and about you from various sources. We limit the collection of Personal Data to what is required to achieve the purpose(s) for which the data was collected.

Directly from you:

- *Data you provide to us:* We obtain Personal Data when contact details are provided to us (e.g., in the context of a contractual business relationship, either by registration on the website, by email or telephone, or by any other means, or when you provide us with your contact details during a business or trade event, or as a candidate in the recruitment process).
- *Relationship data:* We collect or obtain Personal Data in the ordinary course of our contractual relationship with you (e.g., we provide a service to you, or to your employer).

Indirectly from you

- *Security data:* We collect information about your visits to our data center facilities and other premises, including records of the locations accessed and the credentials processed (“data center access records”), and CCTV images captured during your visit to our data centers.
- *Website data:* We may collect or automatically obtain Personal Data when you visit our websites or our Portals, or when you use the features or resources available and associated with our websites.
- *Registration and access details:* We collect or obtain Personal Data when you use, or register to use, our websites, Portals, or services, including records of your interactions with us, such as details of your access to our Portals.
- *Relationship data through your employer or your agent:* We collect or obtain Personal Data from our customers, suppliers and service providers who provide your details to us as your employer or as your agent.

Indirectly through a third-party:

- *Third party information:* We may collect or obtain your Personal Data from third parties including though not limited to credit reference agencies, law enforcement authorities, and marketing firms.
- *Content and advertising information:* If you interact with third-party content or advertising on a website (including third party plugins and cookies) we may receive Personal Data from the relevant third-party provider of that content or advertising.

Children:

Our websites, products and services are not intended for use by minors and Digital Realty does not knowingly collect Personal Data from minors.

(D) We use your Personal Data for the following purposes and processing activities

Processing activities

- *Operating and managing our data center facilities and in the performance of contracted data center services to our customers, including provisioning, implementation of work orders by our suppliers and service providers, customer and technical support services, and allowing access to and/or use of our customer Portals*
- *Financial Management and Administration of contracted services*

Personal Data and purposes

- We obtain your Personal Data for the purpose of managing the relationship with our customers, suppliers, and service providers for performance of the contracted services and the administration thereof. This Personal Data includes:
 - Your name and position in your company
 - Your business contact and employer details (including business email address, business phone number)
 - Your credentials for accessing our Portals and/or systems
 - Work order details (records of work orders placed on our Portals) and other business-related information

- *Security and physical access to our data center facilities, including CCTV recordings, electronic security elements/devices associated with physical access to our data centers including access control systems which process your personal data, access credentials, and any biometric data you may choose to provide for these purposes*

- We obtain your personal data for authentication and identification purposes and to allow you access to our secure data center facilities. This Personal Data includes:
 - Your name, your [government approved] personal identification, your vehicle registration number subject to applicable law
 - Your [business] contact and employer details including email address, and phone and mobile number

- Data center access records, including dates, times, locations of your physical access, and any location data or biometric data subject to local requirements
- CCTV footage and images of you near, entering, or inside our facilities

- *Sales, marketing, and maintenance of our customer relationship, including for communicating with you via any means and for providing you with information about similar products and services in which you may be interested, inviting you to complete surveys, and for obtaining your views about our services*
- *Direct marketing communications sent to you as a prospect regarding our products and services, and upcoming promotions using contact details that you have provided to us, subject to obtaining your prior opt-in consent to the extent required under applicable law and enabling you to unsubscribe from our promotional email list at any time*

- We use your Personal Data for the purpose of managing our business relationship with you as our customer, or as a prospect, as well as for sales and marketing purposes. This Personal Data includes:
 - Your name and position
 - Your [business] contact and employer details, including your email address, and phone and mobile number
 - Information whether you have opted out from receiving emails for [direct] marketing purposes
 - Records of consent you have given, together with date and time, means of consent and any related information (e.g., subject matter of consent)

- *Provisioning (and improving) our websites and Portals and communicating with you in relation to your visit to our websites and Portals; content and advertising, and any other communications with you, including use of cookies and similar tracking technologies in*

- We may automatically collect your personal data in relation to your visit to our websites and Portals, subject to applicable law. This Personal Data includes:
 - Device type, operating system, browser type, browser settings,

accordance with our Cookie Policy (see Section L)

IP address, language setting, dates, and times of connecting to a website

- Records of your interactions with our online advertising and content, any interaction you may have with such content or advertising (e.g., mouse hover, mouse clicks, any forms you complete in whole or in part) and any touchscreen interactions
- Portal usage statistics, Portal settings, dates and times of connecting to a Portal, username, password, security login details, usage data, aggregate statistical information
- Records of consent you have given, together with date and time, means of consent and any related information (e.g., subject matter of consent)

- *Management of IT systems: management and operation of our IT and security systems, and audits (including security audits) and monitoring of such systems*
- *Detecting and investigating criminal offences and breaches (including fraud detection); establishing, exercising, and defending legal rights in the context of legal proceedings; compliance with our legal and regulatory obligations under applicable law*

- We obtain your Personal Data for managing and maintaining our IT systems in compliance with applicable information security frameworks, for investigation purposes and for exercising legal rights and obligations. This Personal Data includes:
 - Your contact and employer details (including business email address and business phone number)
 - Login details, if applicable

- *Health and safety risk assessment and recordkeeping for the purpose of providing a safe and secure environment at our premises and compliance with related legal obligations, subject always to the extent this may be required by applicable law*

- We may obtain your Personal Data in relation to protecting your health and safety, subject to applicable law. This Personal Data includes:

- Your contact and employer details
- Your data center access records, if applicable
- Vaccination or health check records, subject to applicable law

- *Recruitment and job applications, recruitment activities (including interviews), analysis of suitability for relevant positions, records of hiring decisions, offer details and acceptance details*

- We obtain your Personal Data for the purpose of recruitment activities and handling job applications. This Personal Data includes:
 - Your personal contact details (name, surname, postal address, email address, home phone number and/or mobile phone number)
 - Basic information in the recruitment procedure: your curriculum vitae, your application letter, your assessment and/or other information, if applicable
 - Records of consent you have given, together with date and time, means of consent and any related information (e.g., subject matter of consent)

(E) Legal basis for processing your Personal Data

We may process your Personal Data, as described under section (D), based on one of the following legal bases. Such legal basis may depend on the specific context and purpose for which your Personal Data is processed, and subject to applicable law.

Performance of a Contract - We may use your Personal Data to prepare for, enter, and fulfill contractual obligations:

- In the context of our contractual business relationship
- In relation to the performance of the contracted services

Legitimate interests - We may use your Personal Data for our legitimate interests as lawfully allowed, to the extent these legitimate interests are not overridden by your interests, fundamental rights or freedoms (see Section (M)). Such legitimate interests include the following:

- Improving our services
- Providing information to our customers, prospective customers, and other interested parties about our products and/or services
- Ensuring the security of our data center facilities
- Ensuring network and information security
- Preventing and detecting fraud
- For administrative and legal compliance purposes

Your Consent - We may process your Personal Data based on your consent, given voluntary and in an affirmative way. Your consent can be withdrawn at any time. Examples of where we rely on consent include, though are not limited to, the following situations:

- When you opt-in to receive selected marketing communications about our products and services and/or promotional materials
- When you accept the use of cookies and similar tracking technologies when visiting our websites and Portals
- When you are an employment applicant in our recruitment process
- When, as a customer representative, you agree to sharing your business contact details with one or more other customers for business-related purposes

Compliance with a legal obligation - We may use your Personal Data to comply with legal obligations in accordance with applicable law. This includes the following situations:

- For fulfilling our administrative and tax obligations
- For fulfilling our obligations under local health department orders

Protection of vital interests - We may need your Personal Data to protect your interests or the interests of others, such as for the purposes of contacting emergency services in the event of an accident or incident at our data center or office facilities.

(F) Sharing of Personal Data with third parties

We will only share your Personal Data with third party in the following situations:

- We may share your Personal Data with our contracted service providers, suppliers, and other third-party processors, who act on our behalf and only process your Personal Data in accordance with our prior documented instructions. These providers are authorized to use your Personal Data only as necessary to provide us their services. Where we engage any service providers, we take all reasonable and adequate measures to ensure that the confidentiality and security of the Personal Data is protected, together with any additional requirements under applicable laws. The list of processors to whom we disclose Personal Data and the associated purpose [can be found on our website](#).
- We may share your Personal Data with other entities within the Digital Realty group, for legitimate business purposes and for the operation of our websites and providing our services to you, in accordance with our contractual obligations and applicable law.
- We may share your Personal Data with other customers based on your prior consent (e.g., for cross connection purposes within our data center facilities or enabling interaction within the Digital Realty Marketplace).
- We may share your Personal Data in the context of a (potential) business transaction, such as a transaction to buy, sell, merge, or otherwise reorganize our business.
- We may share your Personal Data with legal authorities and external advisors as necessary in connection with legal proceedings, and for investigating, detecting, or preventing criminal offences.
- We reserve the right to disclose your Personal Data to the authorities if required to do so by law, to the extent we believe it is reasonably necessary to comply with applicable law and/or it is in the interest of the rights, property, or safety of our employees, customers, or the public.

Digital Realty does not sell personal data to third parties.

(G) Transfer of Personal Data Internationally, including from the EEA to countries outside of the EEA

Due to the international nature of our business, we may transfer your Personal Data within the Digital Realty group, and to third party Data Processors as noted in Section (F) above for the specific purposes set out under section (D) in this Notice. For this reason, we may transfer Personal Data to other countries that may have different laws and data protection compliance requirements to those that apply in the country in which you are located. We comply with all relevant laws pertaining to the transfer of your personal data between countries to keep your data protected.

Where we transfer your Personal Data from the EEA to recipients located in a country outside the EEA that is not recognized by the European Commission as having an Adequate Jurisdiction, we do so on the basis of the European Commission's Standard Contractual Clauses. The applicable Standard Contractual Clauses set out the rights and obligations for us as the responsible party and for the receiving party to ensure appropriate data protection safeguards for the transfer to the receiving party. They also include specific technical and organizational measures implemented by the receiving party to ensure that the security of the Personal Data will be essentially equivalent to the GDPR requirements (See also under section (H)).

For international data transfers from our UK organization to recipients in non-EEA countries we will use either the ICO's International Data Transfer Agreement (IDTA) or the ICO's International Data Transfer Addendum to European Commission's Standard Contractual Clauses.

You may obtain a copy of our Standard Contractual Clauses using the entity contact details provided in Section (N) below.

(H) Data security

Digital Realty employs appropriate physical, technical, and organizational controls within our organization designed to protect your Personal Data against accidental or unlawful destruction, loss, alteration, or disclosure in accordance with applicable laws and regulations. Our controls are subject to periodic assessment and evaluation by both internal and external auditors. The overall program is evaluated regularly to ensure proper safeguards are in place for the ever-changing cyber environment.

(I) Data accuracy

We take every reasonable step to ensure that:

- Your Personal Data that we Process is accurate, and, where necessary, kept up to date; and
- Where any of your Personal Data that we Process is found to be inaccurate, having regard to the purposes for which the Personal Data is Processed, is erased, or rectified without delay.

From time to time we may ask you to confirm the accuracy of your Personal Data.

(J) Data minimization

We take every reasonable step to ensure that your Personal Data that we Process is limited to the Personal Data reasonably necessary in connection with the purposes set out in this Notice.

(K) Data retention

We will retain your Personal Data for as long as necessary or as permitted by law in relation to the purposes under section (D) for which your Personal Data was obtained. The criteria for determining our retention periods includes:

- The duration of an ongoing business relationship with you
 - Where we provide services and/or carry out a contract with you and/or your employer
 - Where you are lawfully included in our mailing list and have not unsubscribed
- Where we have a legitimate interest in processing the Personal Data for the purposes of operating our business and fulfilling our obligations with you and/your employer
- Where there is a restricted retention period subject to applicable local laws and regulations
 - CCTV recordings for physical security to our data centers
 - Biometric data relating to secure access to data centers
 - Personal information of applicants during the recruitment process (employment law restrictions vary per country)
 - If applicable, any other processing of Personal Data where local laws or regulations requires a restricted retention period
- In compliance with legal obligations to which we are subject per applicable law we have statutory minimum retainment periods
 - e.g., to keep your Personal Data for business records, administrative and tax requirements
- Protecting our legal position
 - To preserve evidence during any applicable limitation period under applicable law (any period during which any person could bring a legal claim against us in connection with your Personal Data, or to which your Personal Data are relevant for defending our interests in the context of judicial proceedings)

Once the retention periods have expired, we will permanently and securely delete, destroy or anonymize the relevant Personal Data.

(L) Cookies and similar technologies

When you visit our website or use one of our Portals, we may place Cookies onto your device, or read Cookies already on your device, subject to obtaining your consent where required, and in accordance with applicable law. We use Cookies to record information about your device, your browser and, in some cases, your preferences and browsing habits. We Process Personal Data through Cookies and similar technologies, in accordance with our [Cookie Policy](#).

(M) Your rights and how you can exercise them

Depending on the applicable data protection and privacy laws, you may have several rights regarding the collection and Processing of your Personal Data, including:

- The right to know whether we process your Personal Data, and if so,
- The right to request access to, or receive copies of, your Personal Data, together with information regarding the nature, purposes of Processing and with whom we have shared your Personal Data.
- The right to request rectification of any inaccuracies in your Personal Data.
- The right to request, on legitimate grounds:
 - The erasure of your Personal Data and/or the right to be forgotten, and
 - Restriction of Processing of your Personal Data (e.g., for direct marketing purposes).
- The right to have certain Personal Data transferred to another Controller, in a structured, commonly used and machine-readable format, to the extent applicable (the right to portability – under the GDPR).
- The right to object to decisions taken solely by computer or other automated processing (including profiling) which produce legal or similarly significant effects on you.
- Where processing of Personal Data is based on consent, the right to withdraw your consent to such processing (note that any withdrawal does not affect the lawfulness of any Processing prior to the date of such withdrawal).
- The right to lodge complaints regarding the Processing of your Personal Data with the competent Data Protection Authority.

- Residents in the EU: the local Data Protection Authority of your EU Member State, or with our leading Data Protection Authority in the EU located in the Netherlands (AP) via its website <https://www.autoriteitpersoonsgegevens.nl>.

(N) How to contact us

To exercise one or more of these rights or to ask a question about these rights or any other provision of this Notice, or about our Processing of your Personal Data, please use the [inquiry form](#) or contact us at any time using one of the below contact details.

Where required by applicable law, we will respond to a valid request relating to your rights within one month of receipt, or within three months where a request is complex and/or requires more time. Please note that:

- In some cases, it will be necessary to provide evidence of your identity before we can give effect to the outlined rights, and
- Where your request requires the establishment of additional facts (e.g., a determination of whether any Processing is non-compliant with applicable law) we will investigate your request promptly.

Contact details

For the purposes of this Notice, the relevant controllers are the affiliates of Digital Realty Trust Inc., including the Interxion EMEA Group.

Regions

Contact details

Americas, Asia-Pacific

privacy@digitalrealty.com

[Telephone: +1 737 281 0101](tel:+17372810101)

Europe, Middle East, and Africa

dpo@Interxion.com

(O) Definitions

- **“Adequate Jurisdiction”** means a jurisdiction that has been formally designated by the European Commission as providing an adequate level of protection for Personal Data.
- **“Cookie”** means a small file that is placed on your device when you visit a website or portal (including our websites and portals). In this Notice, a reference to a “Cookie” includes analogous technologies such as web beacons and clear GIFs.
- **“Controller”** means the entity that determines the purposes and means of Processing Personal Data. In many jurisdictions, the Controller has primary responsibility for complying with applicable data protection laws.
- **“Data Protection Authority”** means an independent public authority that is legally tasked with overseeing compliance with applicable data protection laws.
- **“EEA”** means the European Economic Area.
- **“Personal Data”** means information that is about any individual, or from which any individual is directly or indirectly identifiable, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.
- **“Portal”** means any online portal that provides information or interactive functionality.
- **“Process”, “Processing” or “Processed”** means anything that is done with any Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **“Processor”** means any person or entity that Processes Personal Data on behalf of the Controller (other than employees of the Controller).
- **“Profiling”** means any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.
- **“Standard Contractual Clauses”** means the template transfer clauses adopted by the European Commission or adopted by a Data Protection Authority and approved by the European Commission (latest version EU 2021/914, June 4, 2021).

- **International Data Transfer Agreement (IDTA) and International Data Transfer Addendum (to the Standard Contractual Clauses)** means template transfer clauses adopted by the ICO, the UK's independent Data Privacy Authority and approved by UK Parliament and used as [a] transfer tool for international data transfers to non-EEA countries.

Last updated: March 31, 2022