6 August 2019

Equinix Global Privacy Policy

INTRODUCTION

Equinix (i.e. all entities of the Equinix Group) has adopted this Global Privacy Policy (**Policy**) to ensure that Personal Data is adequately protected when collected, used and/or transferred from one country to another. This Policy establishes a common standard on privacy and Personal Data protection.

Global privacy rules on how Personal Data must be handled within and by Equinix in all countries where Equinix operates

This Policy sets out global rules on how Personal Data must be handled within and by Equinix in all countries where Equinix operates.

It applies to all Equinix entities worldwide and is binding on all such entities and Equinix employees. Equinix will provide appropriate training on this Policy to all its personnel on a regular basis and will also provide adequate information regarding the Policy to all newly hired employees upon their arrival within Equinix. Compliance with all aspects of this Policy will be audited on a regular basis.

The purpose of this Policy is also to regulate the way in which Personal Data relating to individuals is collected, used or otherwise processed, and transferred whether or not by automatic means, within Equinix, to ensure that such Personal Data are adequately protected in accordance with European Data Protection Law.

Global rules that have been approved by European Data Protection Authorities as ensuring adequate protection for Personal Data within Equinix worldwide

Therefore, this Policy, together with the Complaints Handling Policy forms Equinix's Binding Corporate Rules (**BCRs**) as approved by European Data Protection Authorities for providing an adequate level of protection to the Processing of Personal Data by Equinix in accordance with the GDPR which sets out privacy standards for the protection of Personal Data across the European Union.

By complying with the rules and policies set out in these BCRs, transfers of Personal Data relating to European Data Subjects within Equinix globally will be significantly facilitated. This Policy however is not a substitute to any applicable national data privacy laws and regulations in countries where Equinix operates. Local laws will be complied with at all times.

SCOPE

The Policy applies to the Processing of Personal Data by or on behalf of any Equinix entity worldwide and covers transfers of Personal Data from Equinix entities located in the EEA and Switzerland to Equinix entities located in countries outside the EEA or Switzerland.

Binding rules to be complied with by all Equinix employees when handling and transferring Personal Data

This Policy sets out the binding privacy rules and procedures that all Equinix employees must apply and take into account when collecting, holding, using, disclosing, transferring or otherwise handling Personal Data.

Personal Data has a broad meaning and covers all information that directly or indirectly relates to individuals. In some countries (e.g. in Switzerland), data protection rules may also apply to legal persons. Please refer to the definitions provided in Appendix 1 to this Policy.

Personal Data processed by Equinix covers information on its employees and business contacts, such as customers or vendors.

WHO DOES WHAT WITH RESPECT TO THIS POLICY?

Legal departments in each region

Appoint

Regional Privacy Counsel

Who Form

Privacy Office
Comprised of 3 Regional Privacy Counsels and Headed by VP Legal EMEA & Chief Privacy Officer

VP Legal EMEA & Chief Privacy Officer

Privacy Counsel (EMEA)

Privacy Counsel (Asia - Pacific)

Privacy Counsel (USA)

Mission of the Privacy Office:

1. Promote	Compliance with this Policy.
2. Maintain up to date information on	Applicable privacy and data protection laws.
	Personal Data of Equinix's employees and business contacts.
3. Manage	Transfers of Personal Data resulting from business activities.
4. File	Notifications or authorization requests with local data protection authorities and centralize the records of processing.
5. Provide	Notices to (and/or obtain consents where needed from) Data Subjects.
6. Develop	Relationships with other departments within Equinix involved in the implementation of this Policy or in auditing activities relating to this Policy, such as the Business Assurance Services Department (BAS) responsible for performing on a regular basis internal compliance audits covering all aspects of this Policy, including methods of ensuring that corrective actions will take place. Results of the audits will be communicated to the Privacy Office and to the Audit Committee.
7. Receive & handle	Requests and complaints from Data Subjects in relation to their Personal Data.

APPLICABLE PRIVACY RULES FOR THE COLLECTION OF PERSONAL DATA

1.1 Ensure that Personal Data is collected for specific, explicit and legitimate business purposes

Personal Data is generally collected for specific purposes for which it is intended to be used. European Data Protection Law requires that the purpose or reason for which you collect Personal Data must be specific, explicit and legitimate.

As a result, the business purposes for which Equinix may collect Personal Data will be clearly stated, set within certain limits and legally permissible.

To assess whether there is a lawful purpose for collecting Personal Data, you will ensure that **one** of the below conditions is met:

Make sure that you clearly and specifically identify the business need(s) for which Personal Data are collected

- The Data Subject has given consent to the processing of his or her Personal Data by Equinix;

or,

- The Processing of Personal Data is required in order to enter into a contract with the Data Subject or for the performance of the contract with the Data Subject;

or,

- There is a legitimate interest for Equinix to process the Personal Data, provided that this does not cause an unreasonable prejudice to the interests or rights of the Data Subject (for example, for the processing of employees' emergency contacts or for sending direct marketing communications, provided business contacts have means to opt-out according to paragraph 4.2 of this Policy relating to rules for direct marketing);

or,

- The Processing of Personal Data is necessary (i) to protect the Data Subject's vital interest (i.e. in case of a life or death situation), or (ii) to enable Equinix to comply with a legal obligation, or (iii) to perform tasks of public interest (such as administering justice, exercising statutory, governmental or other public functions).

In addition, where Equinix collects data for a specific purpose, it will not use it in a way which is incompatible with the initial purpose.

In some countries, specific rules may also apply if you intend to collect information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, genetic data, or

biometric data for the purpose of uniquely identifying a natural person (Sensitive Data).

Please refer to paragraph 3.4 in relation to how Sensitive Data may be collected.

Equinix processes Personal Data for a number of business purposes including the management of payroll and human resources, the management of customer relationships and the management of vendors/suppliers, notably for the following purposes:

- HR management, such as payroll, disciplinary measures, accounting and employee performance management;
- Negotiation, execution and management of customer contracts;
- Advertising, marketing and public relations;
- Accounts and records, benefits, supply and transaction monitoring;
- Hiring or dismissals of employees;
- Crisis management (for example, to make an inventory and assist employees in case of an act of God); or
- Other purposes required by law or regulation.

1.2 Ensure data accuracy, proportionality and minimisation

Collect Personal Data that is necessary and relevant for the purpose for which you intend to use it

Ensure that Personal Data is kept accurate and up to date & for as long as needed

Personal Data which is collected by Equinix will be adequate, relevant and limited to what is necessary in relation to the business purposes for which it is intended to be used. This requires you to always ensure that there is a clear and foreseeable need for any information collected from an individual in relation to the intended business purpose and that the amount of information collected is proportionate to such business purpose.

Personal Data must be kept accurate, complete, up to date and reliable for its intended use. Thus, Equinix will periodically review the accuracy and completeness of data in its relevant records. Changes to Personal Data about Equinix employees and business contacts will be updated in the relevant records.

Personal Data will only be retained for as long as it is needed to meet the business purposes for which it was collected.

1.3 Ensure Equinix is transparent with Data Subjects on how their Personal Data is collected and used

Ensure that when you collect Personal Data, you notify individuals as to how their data is used in accordance with local law requirements

In countries where information notices are required by relevant local applicable data protection and privacy laws, Equinix will be transparent with Data Subjects by explaining whom and why it collects and uses their Personal Data.

As a result, Equinix will provide information to Data Subjects as to:

- Which Equinix entity is undertaking the Processing of Personal Data (i.e. the "Controller" (please refer to the Definitions provided in Appendix 1 of this Policy));

and,

- The purposes for which Equinix collects Personal Data.

According to what is required by applicable laws and depending on the country concerned, Equinix will also provide information as to:

- The legal basis for the Processing of Personal Data and where the Processing of Personal Data is based on the legitimate interests, the legitimate interests pursued;
- Whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide Personal Data;
- The Recipients or categories of Recipients of the Personal Data;
- The existence of automated decision-making (including profiling) and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing of Personal Data for the individuals;
- The rights of the Data Subjects under this Policy (please refer to sections 4.1, 4.2 and 4.3 of this Policy);
- The period for which the data will be stored or if that is not possible, the criteria used to determine such period;
- The right to lodge a complaint with the competent Data Protection Authority; and
- Any transfers of their Personal Data outside the EEA, Switzerland or outside their country of residence according to local requirements.

You will ensure that such information is given in clear language to the Data Subject upon collection of the Personal Data.

Where Equinix intends to further process the Personal Data for a purpose other than that for which the Personal Data were collected, Equinix will provide the Data Subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in this section.

Where the collection of Personal Data about a Data Subject is performed indirectly (for example, from a publicly available source), Equinix will ensure that the Data Subject is informed of the identity of the Controller handling the data and what it intends to do with such data as soon as practicable upon collection/receipt/retention of such data. According to what is required by applicable laws and depending on the country concerned, Equinix will also in this case inform the Data Subject of the source from which Personal Data originates and of the categories of Personal Data concerned.

Equinix may not provide this information to the Data Subject where Equinix deems it involves a 'disproportionate effort'. In determining what constitutes a 'disproportionate effort', Equinix will evaluate such effort against whether the absence of provision of such information would have a prejudicial effect on the Data Subject.

Equinix will provide the information referred to in this section:

- within a reasonable period after obtaining the Personal Data, but at the latest within one month, having regard to the specific circumstances in which the Personal Data are processed;
- if the Personal Data are to be used for communication with the Data Subject, at the latest at the time of the first communication to that Data Subject; or
- if a disclosure to another recipient is envisaged, at the latest when the Personal Data are first disclosed.

1.4 Rules for collecting Sensitive Personal Data

Ensure that you are entitled to process Sensitive Data

In addition to the rules outlined above and depending on the country where you are located, additional requirements may apply in accordance with applicable data protection and privacy laws where the processing of Sensitive Personal Data is involved; i.e. information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, genetic data, or biometric data for the purpose of uniquely identifying a natural person.

As a rule, under European Data Protection Law, such data should not be collected. However, there are exceptions in specific cases and the collection of Sensitive Personal Data is considered necessary and

relevant for business purposes where **one** of the following conditions is met:

- The Data Subject has given their explicit consent to the processing of their Sensitive Personal Data by Equinix;

or,

- The processing is necessary (i) to allow Equinix to comply with its obligations under employment law, or (ii) to protect the vital interests of the concerned individual or another person where this person is physically or legally incapable of giving their consent (i.e. cases of life and death), or (iii) to establish, exercise or defend a legal claim;

or,

- The Data Subject's Sensitive Personal Data has already been made public.

Please seek advice from your Regional Privacy Counsel to ensure that you are entitled to process Sensitive Personal Data in accordance with any applicable data protection and privacy laws.

APPLICABLE PRIVACY RULES FOR THE USE AND DISCLOSURE OF PERSONAL DATA

1.5 Grant rights of access, rectification, erasure, restriction, objection and right to withdraw consent and data portability to Data Subjects as required under applicable data protection and privacy laws

In several countries where Equinix operates, local data protection and privacy laws may grant Data Subjects certain rights with respect to the processing of their Personal Data, such as the right to access, correct, delete and object to the processing of their Personal Data.

This includes the right for a Data Subject to:

Ensure that individuals can exercise their rights under applicable data protection and privacy laws

- Being informed of whether Equinix holds Personal Data on him/her;
- Request the correction, restriction or deletion of the information that Equinix holds on him/her;
- Object to the processing of their Personal Data by Equinix (including profiling), upon legitimate grounds;
- Request to receive the Personal Data that has been provided to Equinix in a structured, commonly used and machine-readable format, where the processing of such data is based on his consent, or on a contract (Data Portability); and/or

- Where the processing is based on consent, withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

Equinix will inform European Data Subjects of these rights as mentioned in paragraph 3.3 of this Policy. Equinix will also inform Data Subjects in countries where local law provides for such right.

Any written request that you may receive from a Data Subject in relation to their rights (set out above) will be handled as described in Appendix 2 to this Policy. Where the Data Subject makes the request by electronic means, the information will be provided by electronic means where possible, unless otherwise requested by the Data Subject.

Ensure that your Regional Privacy Counsel is informed immediately of any Data Subject's request.

1.6 Grant the right to object to direct marketing

Inform and provide individuals with effective means to opt out from marketing communications in accordance with local law

Equinix may send direct marketing communications to Data Subjects. However, Equinix will abide by any request from a European Data Subject:

- not to use their Personal Data for direct marketing purposes; and
- not to use their Personal Data for profiling to the extent that it is related to such direct marketing.

When sending marketing communications, you will ensure that European Data Subjects are informed of their right to object to their data being used for marketing purposes and provided with means for effectively exercising their opt-out in this regard. In addition, where an individual has asked not to receive marketing communications, you will ensure that it is accurately recorded in relevant databases.

Equinix will also provide for a right to object to direct marketing in countries where local law provides for such right.

1.7 Safeguard against automated individual decisions that are prejudicial

Prevent prejudicial effect as a sole result of automated data processing of data

Decisions that are taken solely based on automated processing of Personal Data (i.e. with no human intervention) may result in decisions having a significant prejudicial effect on the individual.

Equinix will not make decisions that significantly affect a Data Subject solely based on automated processing. Where Equinix does use such decision-making techniques, it will do so according to relevant applicable local law and will observe procedures providing adequate safeguards to protect the legitimate interests of the Data Subject.

In particular, Equinix will comply with the general principle that the Data Subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

By way of exception, this right will not apply if the decision:

a. is necessary for entering into, or performance of, a contract between the Data Subject and Equinix as a Controller;

b. is authorised by EU law or a local law to which Equinix is subject and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests; or

c. is based on the Data Subject's explicit consent.

In the circumstances referred to in points (a) and (c) of the previous paragraph, Equinix shall implement suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of Equinix, to express their point of view and to contest the decision. Additionally, in the circumstances referred to in points (a), (b) and (c) of the previous paragraph, decisions shall not be based on special categories of Personal Data, except under specific conditions provided by applicable law.

1.8 Ensure the security and confidentiality of Personal Data

Where Personal Data is compromised, it may cause serious harm to the individuals and so it follows that adequate measures will be put in place to ensure the security of the use, disclosure and storage of Personal Data.

Ensure that appropriate security measures are in place to protect Personal Data

Equinix will implement appropriate administrative, technical organisational and physical measures to protect Personal Data from loss, theft, misuse and unauthorized access, corruption, disclosure (in particular, where the Processing of Personal Data involves the transmission of data over a network) and against unlawful forms of processing.

These measures will be appropriate to the nature of Personal Data processed and potential identifiable threats.

Equinix employees will receive appropriate information and training relating to the security of Personal Data.

Equinix will disclose Personal Data to third parties only for legitimate purposes and will require such third parties to contractually commit

to providing the same level of privacy and security protection as Equinix.

- External Disclosure: Subject to applicable law, disclosures to law enforcement authorities or regulatory bodies may be carried out by Equinix. In any case, transfers of Personal Data to any public authority cannot be significant, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society;

- Disclosure to Agents and Contractors: Equinix may disclose Personal Data to agents or contractors for the provision of their services to Equinix and this includes processing Personal Data relating to European Data Subjects on Equinix's behalf. In such cases and when European Data Subjects are concerned, Equinix will enter into a contractual agreement with these third parties in compliance with article 28 (1), (2) and (3) of the GDPR, to ensure that they will process such data in accordance with Equinix's documented instructions, will provide appropriate privacy and security protection (as pursuant to this Policy or in conformity with applicable law) and will refrain from any unauthorized use or disclosure of Personal Data.

Upon discovery of any Personal Data Breach relating to European Data Subjects, Equinix employees will notify the Privacy Office of such a Data Breach in accordance with Equinix's Data Breach Management Policy. The Privacy Office will inform Equinix (Services) Limited of such Data Breach. The Privacy Office will also, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the Data Breach to the competent Data Protection Authority. Where the Personal Data Breach is likely to result in a high risk to European Data Subjects' rights and freedoms, the Privacy Office will also notify European Data Subjects of the Personal Data Breach without undue delay. The Privacy Office will maintain a record of all Personal Data Breaches relating to European Data Subjects and will make this record available for inspection by the competent Data Protection Authority.

Further guidance on how to ensure the security of Personal Data is provided in Equinix's IT Security Policy.

1.9 Relationships with Processors that are members of the global corporate group of companies

Where an entity within Equinix's global corporate group of companies processes Personal Data of European Data Subjects on behalf of another entity within Equinix's global corporate group of companies, a written agreement in compliance with article 28 (1), (2) and (3) of the GDPR will be executed requiring the processing entity to:

- Implement appropriate technical and organisational measures to protect the Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or

access, in particular where the Processing of Personal Data involves the transmission of data over a network and against all other unlawful forms of processing;

- Comply with the instructions of the entity on behalf of which the Personal Data is processed and ensure that further sub-processing will not happen without the specific or general authorisation of the controlling Equinix entity;

- Make all reasonable efforts to maintain the Personal Data so that it is accurate and up-to-date;

- Refrain from disclosing the Personal Data to any person except as required or permitted by law or by any written agreement of the entity on behalf of which the Personal Data is processed.

1.10 Transfers of Personal Data outside of a country where Equinix operates into other countries

In circumstances where Personal Data would need to be transferred outside of a country where Equinix operates into other jurisdictions, specific requirements may apply for such a transfer to be permitted.

Ensure that appropriate measures are in place that allow you to carry out a data transfer

Such specific requirements may include: obtaining the prior explicit consent of Data Subjects or providing them with prior notice regarding the transfer of their Personal Data or implementing contractual arrangements in relation to the transfer of the Personal Data.

Please consult your regional Privacy Counsel before any such transfer of Personal Data to determine what needs to be done to carry out such transfer in compliance with applicable data protection and privacy laws.

1.11 Ensure adequate protection when Personal Data of European Data Subjects is transferred to third parties located in countries outside the EEA or Switzerland

European Data Protection Law authorises the transfer of Personal Data to countries outside the EEA or Switzerland **IF** adequate protection is provided to the Personal Data being transferred.

A transfer of Personal Data has a broad meaning and occurs when Personal Data is communicated, moved, accessed or otherwise sent to another country.

Equinix will not transfer Personal Data of European Data Subjects outside of its corporate group of companies to third parties in countries outside the EEA or outside Switzerland, **unless**:

- Those countries have been declared by the European Commission as offering an adequate level of protection for Personal Data;

- Appropriate measures in compliance with European Data Protection Law requirements are in place to ensure the protection and the confidentiality of Personal Data in the countries that do not offer an adequate level of protection. This will be the case where:

    - the Recipient third party is registered on the US Privacy Shield list maintained by the US Department of Commerce; or

    - the Recipient third party concludes, with the relevant exporting entity of Equinix, an agreement based on the EU standard contractual clauses, to ensure the protection of Personal Data.

On an exceptional basis (i.e. only where it is impossible for Equinix to implement the above measures), Equinix may transfer Personal Data of European Data Subjects to a third party located outside the EEA or Switzerland without having to implement the above measures where **one** of the following conditions is met:

- the European Data Subject has given his or her explicit consent to Equinix for the transfer of their Personal Data provided that prior to giving his or her explicit consent, the European Data Subject has been informed of the possible risks of such transfer due to the absence of an adequacy decision and appropriate safeguards; or

- Equinix needs to carry out the transfer of Personal Data to perform or conclude a contract with the European Data Subject; or

- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the European Data Subject between Equinix and a third party; or

- the transfer of Personal Data is necessary: (i) to protect the European Data Subject's vital interests (i.e. in case of a life or death situation), (ii) to allow Equinix to establish, exercise or defend a legal claim or (iii) for important reasons of public interest as recognised in Union law or in the law of the Member State to which the Controller is subject; or

- the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State

law for consultation are fulfilled in the particular case. This transfer will not involve the entirety of the Personal Data or entire categories of the Personal Data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer will be made only at the request of those persons or if they are to be the recipients.

In any case, the transfers of Personal Data relating to European Data Subjects in reliance on the above derogations will be occasional and non-repetitive.

ACCOUNTABILITY

European Data Protection Law requires Equinix to be responsible for, and be able to demonstrate, compliance with the BCRs.

All Equinix Entities within the corporate group of companies have the duty to maintain a record of processing activities. The Privacy Office has the responsibility of maintaining the records of processing activities on behalf of the Equinix Entities. If you intend to carry out a new data processing operation, you will need to inform the Privacy Office in order to allow the record of processing to be updated or a new record of processing activity created. Equinix will make any such record available for inspection by the competent Data Protection Authority.

Where required, data protection impact assessments will be carried out for processing operations that are likely to result in a high risk to the rights and freedoms of European Data Subjects. Where the risks identified in the data protection impact assessment cannot be sufficiently addressed (i.e. the residual risks remain high), the competent Data Protection Authority will be consulted.

European Data Protection Law also requires Equinix to take appropriate technical and organisational measures to implement data protection principles into the Processing of Personal Data relating to European Data Subjects and to ensure that, by default, only Personal Data which is necessary for the purpose(s) for which they are collected, is processed (data protection by design and by default). For each new project/system/application/tool involving the Processing of Personal Data relating to European Data Subjects, you will need to complete Equinix's Privacy by Design Assessment Form.

Compliance with this Policy will be audited by the Business Assurance Services Department on a regular basis and at least every other year or otherwise at the initiative of the Privacy Office, the Legal team and/or the Business Assurance Services Department. The audit programme will cover all aspects of this Policy, including methods of ensuring that corrective actions will take place. Results of the audit will be drawn by the Business Assurance Services Department and communicated to the Privacy Office and to the Audit Committee for

information and review, and, upon request, to the competent Data Protection Authorities.

COMPLAINTS MECHANISM

Equinix will take appropriate measures to ensure that the provisions of this Policy are enforced in accordance with its Complaints Handling Policy.

If a Data Subject has a concern as to whether this Policy may have been breached, the Data Subject may report such concern to one of the Regional Privacy Counsels, without prejudice to the right of the Data Subject to bring a claim before a competent Data Protection Authority or Court.

The Regional Privacy Counsel will acknowledge receipt of the complaint or request to the Data Subject within 5 business days, investigate the complaint or request and shall provide a response to it, including the implementation of any relevant remedial actions, without undue delay and in any event, within one month.

That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Regional Privacy Counsel shall inform the Data Subject of any such extension within one month of receipt of the complaint or request, together with the reasons for the extension.

Where appropriate, the Regional Privacy Counsel may delegate the handling of the complaint or request to the relevant department or individual within the Equinix organization. In such a case, the Regional Privacy Counsel will act as a point of contact for the Data Subject and the person designated to handle the complaint or request and will inform the Data Subject of the outcome of his/her complaint or request.

In most critical and severe cases, i.e. cases of serious Personal Data Breaches, the three Regional Privacy Counsels will meet to handle the complaint or request. Examples of serious events of Personal Data Breaches are those involving (i) a significant number of Data Subjects located across different countries, and/or (ii) cases of non-compliance with the Policy that triggers high risks for the data protection and privacy rights of individuals concerned, and/or (iii) a significant violation of data transfer rules, and/or (iv) a significant unauthorized disclosure of or access to Personal Data belonging to European Data Subjects, and/or (v) serious Personal Data Breaches in relation to direct marketing campaigns, and/or (vi) Personal Data Breaches involving global databases.

Responses to requests and complaints dealt with by the Privacy Office shall be provided under the same timescales as those mentioned above.

A copy of Equinix's Complaints Handling Policy can be made available to Data Subjects upon request to your Regional Privacy Counsel.

CASES WHERE NATIONAL LEGISLATION PREVENTS EQUINIX FROM COMPLYING WITH THE BCR

If you have reasons to believe that there is an applicable local law that prevents Equinix or an Equinix entity from fulfilling its obligations under the BCRs or has substantial adverse effect on the guarantees provided by the BCRs, you will need to promptly inform your Regional Privacy Counsel and/or the Privacy Office (unless otherwise prohibited from such a disclosure, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

In addition, where an Equinix entity is subject to an applicable local law in a Relevant Country that is likely to have a substantial adverse effect on the guarantees provided by the BCRs, you will need to inform your Regional Privacy Counsel and/or the Privacy Office, who can then facilitate a report of the problem to the competent Data Protection Authority. This includes any legally binding request for disclosure of Personal Data by a law enforcement authority or state security body. In its report to the competent Data Protection Authority, the Regional Privacy Counsel and/or the Privacy Office will describe the request it has received, including information about the Personal Data requested, the requesting body and the legal basis for the disclosure (unless otherwise prohibited from such a disclosure, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

If in specific circumstances Equinix is prohibited from suspending the disclosure of Personal Data whilst reporting the problem to the competent Data Protection Authority and/or is prohibited from reporting the problem to the competent Data Protection Authority, the Equinix entity which received this request will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible and be able to demonstrate that it did so. If the relevant Equinix entity, despite having used its best efforts, is not in a position to report to the competent Data Protection Authority, it will provide general information on the requests it received to such competent Data Protection Authority on an annual basis (For example, the number of applications for disclosure, the type of data requested and details of the requester (if possible)).

APPLICATION OF PRIVACY RULES TO EUROPEAN DATA SUBJECTS AND THIRD PARTY BENEFICIARY RIGHTS

1.12 Application of privacy rules to European Data Subjects whose Personal Data has been transferred outside of the EEA and Switzerland

The privacy rules mentioned in paragraphs 3 to 7 and in paragraphs 9 and 10 of this Policy apply not only to European Data Subjects

whose personal data remains in the EEA or Switzerland, but also to European Data Subjects whose Personal Data has been transferred from the EEA and Switzerland and are processed outside the EEA or Switzerland by Equinix entities bound by this Policy.

1.13 Third party beneficiary rights

European Data Subjects whose Personal Data is transferred from the EEA or Switzerland and who complain of a breach of one or more of the principles enforceable as third party rights listed below may invoke this Policy and lodge a complaint against Equinix (Services) Limited in the United Kingdom and/or bring an action before:

- the Courts in the country of the EEA or in Switzerland where the data exporter has an establishment; or
- the Courts in the country of the EEA or in Switzerland where the European Data Subject has his or her habitual residence; or
- the Data Protection Authority in the country of the EEA or in Switzerland where the European Data Subject has his or her habitual residence or place of work, or where the European Data Subject considers that the alleged infringement has occurred.

A European Data Subject whose Personal Data is transferred from the EEA or Switzerland is entitled to compensation directly from Equinix (Services) Limited in the United Kingdom for the damage suffered, where he or she has established that he or she has suffered damage as a result of a breach of one or more of the principles enforceable as third party rights listed below, in accordance with the conditions of applicable liability law.

The principles which are enforceable by European Data Subjects whose Personal Data is transferred from the EEA or Switzerland as third party beneficiary rights are as follows:

- Purpose limitation;
- Data minimisation and accuracy;
- Limited storage periods;
- Processing of special categories of personal data;Data quality and proportionality;
- Legal basis for processing; Transparency, fairness and lawfulness, and easy access to BCR;
- Rights of access, rectification, erasure, restriction of data and object to the Processing of Personal Data;

- Rights where individual decisions solely based on automated processing are taken;

- Responsibility for and ability to demonstrate compliance with the BCRs, in particular by:

    - Maintaining a written record of all categories of processing activities carried out, which should be made available to the competent Data Protection Authority on request;

    - Carrying out a data protection impact assessment for processing operations that are likely to result in a high risk to the rights and freedoms of natural persons and consulting the competent Data Protection Authority whenever the assessment indicates that the processing would result in a high risk.

- Data protection by design and by default;

- Security and confidentiality, including the obligation to enter into a contractual agreement with Agents and Contractors in compliance with article 28 (1), (2) and (3) of the GDPR as well as the duty to notify Personal Data Breaches to Equinix (Service) Limited and also to notify the Personal Data Breach to the competent Data Protection Authority. Where the Personal Data Breach is likely to result in a high risk to European Data Subjects' rights and freedoms, the Privacy Office will also notify European Data Subjects of the Personal Data Breach without undue delay;

- Restrictions on transfers and onward transfers outside of the Equinix corporate group of companies;

- National legislation preventing compliance of the BCRs;

- Right to complain through the internal complaint mechanism of the Equinix corporate group of companies;

- Cooperation duties with Data Protection Authorities; and

- Liability and jurisdiction provisions

DATA SUBJECTS' RIGHT TO HAVE EASY ACCESS TO THE BCRS

Data Subjects have a right to easily access Equinix's BCRs which is comprised of this Policy and the Equinix Complaints Handling Policy.

Equinix will ensure that the BCRs are made available to Data Subjects via its intranet and external website(s).

RELATIONSHIP BETWEEN NATIONAL LAWS AND BCRS

The GDPR determines which law applies to the processing of Personal Data relating to European Data Subjects.

Where an applicable local law requires a higher level of protection of Personal Data than is provided for in this Policy, Equinix will comply with the applicable local law, which will take precedence over this Policy.

In case of a conflict between an applicable local law and this Policy, the Regional Privacy Counsel and/or the Privacy Office will decide on which action to take and will consult with the competent Data Protection Authority, where necessary.

FINAL PROVISIONS

Effective date: This Policy will become effective as of 22 October 2019.

No transfer of Personal Data will be made on the basis of the BCRs until all the commitments are fully implemented between the importers and exporters. If a transfer of Personal Data relating to European Data Subjects takes place during the transition period, the transfer will be made on the basis of another tool providing adequate safeguards (For example, standard contractual clauses).

If you have any queries about this Policy, please contact VP Legal and Chief Privacy Officer at privacyoffice@eu.equinix.com.

APPENDIX 1 - DEFINITIONS

In this Policy, the following terms shall mean:

"Binding Corporate Rules" means this Policy and the Complaints Handling Policy, to which Equinix is bound to ensure an adequate level of protection for European Data Subjects' Personal Data Transfers from the EEA or Switzerland.

"Controller": any Equinix entity which alone or jointly with others determines the purposes and means of the Processing of Personal Data.

"GDPR": Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), which provides for the protection of Personal Data in the European Economic Area.

"European Data Protection Law": Body of laws comprising the GDPR and national data protection laws in the EEA and Switzerland

"Data Subject": any identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. As such, Data Subjects include employees (current or former employees, free-lancers, consultants, agents, temporary workers, trainees hired by Equinix), applicants, customers, correspondents, advisers, vendors, suppliers and contact persons of Equinix - whose Personal Data is processed by or on behalf of any Equinix Entity.

"European Data Subjects" means a Data Subject whose processing of his or her Personal Data falls under the scope of the GDPR or under the scope of the Swiss data protection law;

"Personal Data": any information relating to an identified or identifiable natural person (a "Data Subject"). In some countries (for example, Switzerland) data protection rules also apply to identified or identifiable legal persons.

"Personal Data Breach": a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"Processor" (service provider): the legal entity which processes personal data on behalf of Equinix acting as the Controller;

"Equinix": all entities of the Equinix Group worldwide.

"Processing of Personal Data": any operation or set of operations performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Recipient": a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.

“Relevant Countries” means the countries other than those included in the European Economic Area and countries in respect of which the European Commission has not issued an adequacy finding under Article 45 of the GDPR.

“Sensitive Personal Data”: Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and information concerning health, sex life or sexual orientation, genetic data, or biometric data for the purpose of uniquely identifying a natural person.

“Third Party”: any natural or legal person, public authority, agency or body other than the Data Subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, are authorised to process the data.

“Transfer” means transferring or making available Personal Data to any another entity by any means.

APPENDIX 2 – COMPLAINTS HANDLING POLICY

6 August 2019

EQUINIX COMPLAINTS HANDLING POLICY

The purpose of this Policy is to set out the procedure which applies to all Equinix entities when a data subject exercises any of its applicable rights under local data protection and privacy laws and regulations and/or under the Equinix Global Privacy Policy. Specifically, this Policy relates to the registration of complaints regarding Equinix or where individuals make requests for access and other related rights regarding personal data that Equinix may hold in relation to them.

All the terms used in this Policy shall have the meaning set out in Appendix 1 of Equinix Global Privacy Policy.

This Policy applies to European Data Subjects whose personal data remains in the EEA or Switzerland and to European Data Subjects whose Personal Data has been transferred from the EEA and Switzerland and is processed outside the EEA or Switzerland.

Equinix and its employees must take appropriate measures to ensure that the provisions of the Global Privacy Policy are complied with.

The Privacy Office, led by VP Legal EMEA and Chief Privacy Officer, consists of three Regional Privacy Counsels covering:

(EMEA) (Asia-Pacific) (USA)

A data subject may, from time to time, exercise rights afforded to certain individuals under applicable data protection and privacy laws and regulations (including but not limited to, the European Union's General Data Protection Regulation (GDPR)) by contacting the Equinix Privacy Office and specifically, the relevant Regional Privacy Counsel.

A data subject means employees, customers, suppliers, vendors or contact persons of Equinix: any such persons may report any concerns about compliance with the Global Privacy Policy or exercise applicable rights, as scoped and set out in this Policy.

Any Equinix employee who is informed of such (1) a concern or a complaint and/or (2) a data subject access request or similar in relation to a data privacy matter, must immediately forward it to the Regional Privacy Counsel for investigation and resolution.

In each case, a concern or complaint or a data subject access request that is made that is in scope of the parameters of this Policy will be registered and recorded by the Privacy Office. A full record of all such issues raised and resolved shall be maintained by the Privacy Office.

Each Regional Privacy Counsel is responsible for reviewing, processing and responding to all complaints from data subject and data subject access requests in the applicable region, as set out in this Policy. Where appropriate, the Regional Privacy Counsel will be assisted by other departments, including Human Resources, which may be involved in the review and response, depending on the nature of the matter.

1. COMPLAINTS HANDLING PROCEDURE

The Privacy Office will act as a forum for the handling of data protection breaches, at the discretion of the Regional Privacy Counsel, but in any event, in relation to all instances of serious events of data protection breaches.

Serious events of data protection breaches are, for example, those involving (i) a significant number of data subjects located across different countries; and/or (ii) instances of non-compliance with the Global Privacy Policy that triggers high risks for the data protection and privacy rights of the individuals concerned; and/or (iii) a significant violation of data transfer rules; and/or (iv) a significant unauthorized disclosure of, or access to, personal data relating to European Data Subjects ("European Data Subjects" means a Data Subject whose processing of his or her Personal Data falls under the scope of the GDPR or under the scope of the Swiss data protection law); and/or (v) serious breaches of direct marketing campaigns; and/or (vi) cases involving global databases.

Once a complaint is received by the Privacy Office, the Regional Privacy Counsel will acknowledge receipt to the data subject within 5 business days and will open a case-file (electronic or manual) for each complaint related to breaches of the Global Privacy Policy. The file will contain the relevant documentation, including correspondence with the data subject. The Regional Privacy Counsel will maintain the file.

The Regional Privacy Counsel will keep a log of the complaints made. The Regional Privacy Counsel will report to the Privacy Office on a regular basis with a view to take corrective actions if needed and improve guidelines and procedures to be implemented within Equinix.

Where appropriate and depending on the nature of the breach, the Regional Privacy Counsel may delegate the handling of the complaint to the relevant department or individual within the Equinix organization. In such circumstances, the Regional Privacy Counsel will act as a point of contact for the data subject as the person designated to handle the complaint and will inform the data subject of the outcome of their complaint.

If the complaint is upheld by Equinix, then Equinix will implement appropriate remedial measures. Those measures will be decided on a case by case basis by the Regional Data Privacy Counsel and, where applicable, any other relevant department.

In any event, data subjects shall be provided with a response to their complaint, including through the implementation of any remedial actions, within a maximum period of 1 month of receipt of the complaint, unless a shorter maximum period applies under applicable data protection and privacy laws.

That period may be extended by 2 further months where necessary, taking into account the complexity and number of the requests, in compliance with applicable data protection and privacy laws.

These response timescales also apply to complaints that are dealt with by the Privacy Office.

The Privacy Office will meet at least on an annual basis to review all complaints and how they were handled and resolved.

2. SPECIFIC REQUESTS ON RIGHTS OF ACCESS, RECTIFICATION, ERASURE, RESTRICTION, WITHDRAW OF CONSENT, OBJECTION AND PORTABILITY ACCORDING TO APPLICABLE LOCAL DATA PROTECTION AND PRIVACY LAWS

2.1 The rights of access, rectification, erasure, restriction, withdraw of consent, objection and portability

The following applies to requests concerning the rights of access, rectification, erasure, restriction, withdraw of consent, objection and portability, where such rights are provided for by local applicable data protection and privacy laws (e.g of the country where the data subject is located or of the country where his/her personal data are processed (employee, customer, supplier, vendor, contact person of Equinix)) and to requests from European Data Subjects whose personal data has been transferred from the European Economic Area and Switzerland.

2.1.1 Nature of the rights

In several jurisdictions, local data privacy legislation and regulations provide that data subjects have a right to access personal information processed about them. If Equinix processes such information, the data subject may request a copy of such information.

According to such local laws, data subjects may also request the rectification of such information if it is found to be incomplete and/or inaccurate. Data subjects may also request Equinix to erase personal information without undue delay if certain conditions are met.

Data subjects have the right to object to the processing of their personal data by Equinix under local applicable laws. When such data is processed for direct marketing purposes, the objection may be made upon request and free of charge. When such data is processed for other purposes, the data subject has the right, in accordance with applicable data privacy laws and regulations, to object to such processing on the basis of compelling legitimate reasons.

Data subjects have the right to obtain from Equinix the restriction of the processing of their personal data under local applicable laws.

Data subjects also have the right under local applicable laws to receive the personal data concerning them, which they have provided to Equinix, in a structured, commonly used and machine-readable format and the right to ask Equinix to transmit that data to another data controller.

Equinix will also provide the above-mentioned rights to data subjects whose personal data has been transferred from the European Economic Area.

2.1.2 Who can make a request?

Requests may be made by all data subjects including employees, customers, suppliers, vendors and contact persons of Equinix, provided that their personal data is processed by Equinix in jurisdictions where local applicable data protection laws provide for rights of access, rectification, erasure, restriction, withdraw of consent, objection and portability or

whose personal data has been transferred from the European Economic Area. The data subject (or their authorised representative where permitted in accordance with applicable laws), can only make a request in respect of personal data relating to themselves: it is strictly a personal right.

2.1.3 **Response time**

The Regional Privacy Counsel will acknowledge receipt of the data subject's request within 5 business days and respond to a request within 1 month of receipt of the request unless a shorter maximum period is set under applicable local data protection laws and regulations.

That period may be extended by two further months, where necessary, taking into account the complexity and number of requests. Equinix shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Responses to requests that are dealt with by the Privacy Office shall be provided under the same timescales as those mentioned above.

2.2 **Procedure for responding to requests from data subjects**

The Regional Privacy Counsel will review, process and respond to all requests within the timeframe required by applicable local data privacy legislation and regulations.

If an Equinix employee receives a request from any data subject wishing to exercise their rights, that employee must immediately forward such request to the Regional Privacy Counsel and/or the Privacy Office.

The Regional Privacy Counsel will open a case-file (electronic or manual) for each request from a data subject seeking to exercise their rights under the applicable data privacy legislation and regulations. The file will contain the relevant documentation, including correspondence with the data subject. The Regional Privacy Counsel will maintain the file as part of their duties.

The Regional Privacy Counsel will keep a log of the number and type of requests made by data subjects. The Privacy Counsel shall report to the Privacy Office on a regular basis, with a view to take corrective actions, if needed and improve guidelines and procedures to be implemented within Equinix.

Where the data subject makes the request by electronic form means, the information will be provided by electronic means where possible, unless otherwise requested by the data subject.

2.2.1 **Exercise of the right of access**

In making a request for access, the data subject (as defined above in 2.1.2) will need to provide sufficient information to enable the Regional Privacy Counsel to identify the data subject.

The data subject concerned has a right to request the following:

- to know whether Equinix processes personal data concerning them;
- the purposes for which such data is processed;

- the categories of data undergoing processing;

- the recipients or categories of recipients of such data;

- where possible, the envisaged period for which personal data will be stored or if not possible, the criteria used to determine that period;

- the existence of the right to request from Equinix rectification or erasure of personal data or restriction of processing data concerning the data subject or to object to such processing;

- the right to lodge a complaint with a supervisory authority;

- where the personal data is not collected from the data subject, any information available as to how the data was collected (i.e. the source); and

- a copy of the actual data processed about them.

Where provided by the local applicable law of the country where the data subject is located or of the country where his/her personal data are processed, if such processing of personal data may result in automated decisions, the request for access may also cover the existence of automated decision-making, including profiling and meaningful information about the logic involved in such automatic processing of data concerning the data subject, as well as the significance and the envisaged consequences of such processing for the data subject.

The Regional Privacy Counsel will consider and respond to a valid request from a data subject to access their personal data as follows:

a) The Regional Privacy Counsel will ask the data subject making a request to prove their identity, for example, by providing a copy of their personnel number, ID or any other satisfactory document to verify the data subject's identity.

b) The Regional Privacy Counsel may request the data subject concerned to supply any additional information as may be necessary or desirable to better define their request or to help Equinix locate the relevant data, in particular where the requested data relates to Equinix's electronic mail systems.

c) The Regional Privacy Counsel will assess if the request falls within the scope of any exemptions from the right of access provided for by the applicable data privacy laws and regulations or other applicable country laws. The Regional Privacy Counsel will also assess whether the request is abusive based on the frequency, the number and the repetitive or systematic nature of the requests and can decide not to respond to such requests unless required by local law. If this is the case, the Regional Privacy Counsel will fully document any decision to withhold the data on the basis of an exemption provided in the applicable data privacy laws or other applicable country laws. This will form part of the access request case-file, as described in Section 2.2 above.

d) The Regional Privacy Counsel will where relevant contact the relevant Equinix departments and functions likely to process personal data concerning the data subject. Such departments and functions will co-operate with the Regional Data Privacy Counsel and supply any necessary information and data as the Regional Data Privacy Counsel deems appropriate.

e) Once the Regional Privacy Counsel is satisfied that it has obtained all useful and complete information, the Regional Privacy Counsel will ensure that the data disclosure does not infringe the data privacy rights of another data subject.

f) Where the information to be provided as a result of an access request contains data about another data subject, the Regional Privacy Counsel will provide the requested information only if:

- it is possible to delete or conceal the data identifying the other data subject; or

- the other data subject has consented to such a disclosure; or

- in cases where a consent has not been sought or has proven impossible to obtain and where it is impracticable to delete or conceal the data identifying the other data subject, the Regional Privacy Counsel determines that under the circumstances of that particular case it is appropriate and reasonable to provide the data.

The Regional Privacy Counsel will fully document any considerations and decisions in this respect and include it in the case-file described in Section 2.2 above.

g) The data to be provided to the data subject must be presented in an intelligible form. Any codes used must be clearly explained and the data translated in a language comprehensible to the data subject concerned.

h) The requested data will be provided to the data subject concerned in a written form or where agreed, the data subject will be given the opportunity of viewing the requested data.

2.3 **Exercise of the right of rectification**

The data subject (as defined above in 2.1.2) may request that the personal data processed about them by Equinix be corrected where they consider such data to be inaccurate or incomplete.

On receipt of such a request, the Regional Privacy Counsel should verify that, taking into consideration the information communicated by the data subject concerned, the data processed is actually inaccurate or incomplete. The data subject making such request must provide appropriate documentation to the satisfaction of the Regional Privacy Counsel to substantiate such correction request.

If the verification process shows that the data is actually inaccurate or incomplete, the Regional Privacy Counsel will instruct the relevant department or function to correct or complete the data. If the verification process shows that the data in question to be accurate, the Regional Privacy Counsel shall make a note of the findings and communicate this to the data subject.

When the information has been rectified, the department or function will send a copy of the rectified data to the Regional Privacy Counsel who, in turn, will forward this to the data subject concerned to confirm that their request has been considered and where appropriate, processed.

Where it is determined that incorrect and/or incomplete information was communicated to other Equinix and/or third party entities, the Regional Privacy Counsel will instruct the relevant department or function to communicate the rectified data to those entities for correction, unless such operation is impracticable or involves a disproportionate effort.

2.4 **Exercise of the right to erasure**

The data subject (as defined above in 2.1.2) may request that the personal data processed about them by Equinix be erased where one of the following grounds applies:

a) the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;

b) the data subject withdraws consent and there is no other legal ground for the processing;

c) the data subject objects to the processing of their personal data where the processing is based either on a public interest ground or on the legitimate interests of Equinix and there are no overriding legitimate grounds for the processing;

d) the data subject objects to the processing of their personal data where they are processed for direct marketing purposes;

e) the personal data have been unlawfully processed;

f) the personal data has to be erased for compliance with a legal obligation in the legislation of a country to which Equinix is subject; or

g) the personal data has been collected regarding children in the context of information society services.

By way of exception, the data subject may not obtain the erasure of their personal data where the processing of their personal data is necessary:

a) for exercising the right of freedom of expression and information;

b) for compliance with a legal obligation which requires processing;

c) for reasons of public interest in the area of public health;

d) for archiving purposes in the public interest, scientific or historical research purpose; or

e) for the establishment, exercise or defence of legal claims.

In these cases, Equinix is not obliged to erase the personal data relating to the data subject.

On receipt of such a request, the Regional Privacy Counsel should verify that, taking into consideration the information communicated by the data subject concerned, one of the above-mentioned grounds applies. The data subject making such request must provide appropriate documentation to the satisfaction of the Regional Privacy Counsel to substantiate such erasure request.

If the verification process shows that one of the above-mentioned grounds applies, the Regional Privacy Counsel will instruct the relevant department or function to erase the data. If the verification process shows that none of the above-mentioned grounds applies or that Equinix has a legitimate reason not to erase the data (i.e. Equinix falls within one of the five above–mentioned exceptions), the Regional Privacy Counsel shall make a note of the findings and communicate this to the data subject.

When the information has been erased, the department or function will notify the Regional Privacy Counsel who, in turn, will confirm to the data subject concerned that their request has been considered and that the data has been erased.

Where it is determined that the data subject's personal data was communicated to third party entities, the Regional Privacy Counsel will instruct the relevant department or function to notify these third party entities the erasure of that data, unless such operation is impracticable or involves a disproportionate effort.

2.5 **Exercise of the right to restriction of processing**

The data subject (as defined above in 2.1.2) may request from Equinix the restriction of the processing of their personal data where one of the following conditions applies:

a) the data subject contests the accuracy of the personal data for a period; the restriction of the processing will enable Equinix to verify the accuracy of the personal data;

b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of its use instead;

c) Equinix no longer needs the personal data for the purposes of the processing, but such personal data is required by the data subject for the establishment, exercise or defence of legal claims; or

d) the data subject has objected to processing on grounds relating to their particular situation pending the verification whether the legitimate grounds of Equinix override those of the data subject.

On receipt of such a request, the Regional Privacy Counsel should verify that, taking into consideration the information communicated by the data subject concerned, one of the above-mentioned conditions applies. The data subject making such request must provide appropriate documentation to the satisfaction of the Regional Privacy Counsel to substantiate such restriction request.

If the verification process shows that one of the above-mentioned conditions applies, the Regional Privacy Counsel will instruct the relevant department or function to restrict the processing of the data. If the verification process shows that none of the above-mentioned conditions applies, the Regional Privacy Counsel shall make a note of the findings and communicate this to the data subject.

When the processing of the personal data has been restricted, the department or function will notify the Regional Privacy Counsel who, in turn, will confirm to the data subject concerned confirm that their request has been considered and that the processing has been restricted.

Where it is determined that the data subject's personal data was communicated to third party entities, the Regional Privacy Counsel will instruct the relevant department or function to notify these third party entities the restriction of the processing of that data, unless such operation is impracticable or involves a disproportionate effort.

2.6 Exercise of the right to object

2.6.1 Right to object to direct marketing

The data subject (as defined above in 2.1.2) has the right to object to receiving any promotional and marketing materials by post, telephone, email or any other form of communication provided by Equinix. The data subject also has a right to object to Equinix processing their data (which includes profiling) for any direct marketing purposes.

Upon receipt of such an objection, the Regional Privacy Counsel will ask the departments or functions concerned to cease using the data subject's data for direct marketing purposes.

The procedure described in the above paragraphs shall be repeated here as well.

2.6.2 Right to object on grounds relating to the data subject's particular situation

Equinix will abide by any justified request from a data subject (as defined above in 2.1.2) to stop the processing of their data, if the data subject objects to the processing of personal data concerning them which is based either on a public interest ground or on the legitimate interests of Equinix on grounds specific to that data subject's situation and where Equinix has no legitimate grounds which override those of the data subject.

The procedure described in the above paragraphs shall be repeated here as well.

2.7 Exercise of the right to portability

Equinix will abide by any justified request from a data subject (as defined above in 2.1.2) to exercise its right to portability.

The right of portability is composed of:

- a right for the data subject to receive from Equinix their personal data which they have provided to a controller, which the controller must provide that data in a structured, commonly used and machine-readable format.

- a right for the data subject to transmit that data to another controller

The right to portability applies when the following conditions are met:

- the processing is based on consent or on the performance of a contract or pre-contractual measures; and

- the processing is carried out by automated means.

If the right of portability applies (i.e. if the above conditions are met):

- Equinix must provide, in a structured, commonly used and machine-readable format, the following data:

    - Data actively and knowingly provided by the data subject (for example, mailing, address, age, etc.); and

    - Observed data provided by the data subject by virtue of the use of a service or a device.

In contrast, inferred data and derived data which are created by the Equinix on the basis of the data provided by the data subject are not within the scope of the right to data portability.

The procedure described in the above paragraphs shall be repeated here as well.

2.8 **Exercise of the right to withdraw consent**

Where processing is based on consent, the data subject (as defined above in 2.1.2) has the right to withdraw consent by post, telephone, email or any other form of communication provided by Equinix. It must be as easy to withdraw as to give consent.

Upon receipt of such a withdrawal, the Regional Privacy Counsel will ask the departments or functions concerned to cease using the data subject's personal data. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

The procedure described in the above paragraphs shall be repeated here as well.

If you have any query about this Policy, please contact the Equinix Privacy Office at privacyoffice@eu.equinix.com.

APPENDIX 3- LIABILITY

In such circumstances where Personal Data of a European Data Subject is transferred by an Equinix entity in the European Economic Area (EEA) or Switzerland, to an Equinix entity located outside of the EEA or Switzerland and where the European Data Subject complains that a breach of this Policy has occurred in relation to the handling of his or her Personal Data, Equinix (Services) Limited in the United Kingdom will:

- Ensure that the necessary actions to remedy breaches to the Policy by the relevant Equinix entity based outside of the EEA or Switzerland are implemented;

- Bear the burden of proof to establish that the Equinix entity based outside of the EEA or Switzerland was not responsible for the Policy breach and/or that no such Policy breach took place, should the case arise (assuming that the European Data Subject can demonstrate that he/she has suffered damage and establish facts which show it is likely that the damage has occurred because of the Policy breach).

Where applicable and relevant, Equinix (Services) Limited will:

- defend the lawfulness of the processing via all available means (including in attendance with the relevant Data Protection Authority); and

- Pay compensation for any damages suffered by the European Data Subject resulting from a Policy breach by an Equinix entity without any ambiguity and with all required evidence, should the case arise.

Where applicable, the Equinix entity located outside of the EEA or Switzerland will provide Equinix (Services) Limited with all documentation (correspondence, files, records, etc) that is necessary for the defence of such a claim.

Should Equinix (Services) Limited be held liable for a Personal Data Breach, the importing Equinix entity based outside of the EEA or Switzerland, will indemnify it for any and all costs, damages, expenses or losses it has incurred.

In the event the United Kingdom leaves the European Union and ceases to be a member of the EEA, Equinix EMEA B.V in the Netherlands will take over all the obligations of Equinix (Services) Limited described above.

APPENDIX 4 - MUTUAL ASSISTANCE AND COOPERATION WITH DATA PROTECTION AUTHORITIES

Equinix will co-operate with Data Protection Authorities in the EEA and Switzerland and other relevant regulators where required by applicable local law.

All Equinix entities will file the notifications, authorisations and other specific procedures with the competent Data Protection Authority in the EEA and Switzerland where required by applicable local law.

All Equinix entities will co-operate and assist each other in order to respond in a reasonable time period to any relevant query from the competent Data Protection Authority in the EEA and Switzerland and will agree to be audited by a Data Protection Authority in the EEA and Switzerland in accordance with their applicable audit procedures. Upon request, they will communicate to the competent Data Protection Authorities in the EEA and Switzerland the results of previous audits. They will co-operate with the competent Data Protection Authorities in the EEA and Switzerland in relation to any decision made by such authorities.

APPENDIX 5 - UPDATE OF THE RULES

Equinix will ensure that this Policy and subsequent updates are made available to its employees, customers and vendors (for example, via its intranet and website).

The Privacy Office of Equinix in the EEA, which is headed by VP Legal, EMEA will:

- maintain an up-to-date list of all amendments to this Policy and of all Equinix entities that are required to comply with this Policy;

- notify all Equinix entities of changes to this Policy;

- inform all employees, customers and suppliers in relation to whom Personal Data is being processed of any substantial changes to this Policy and

- report once a year any changes to this Policy or any changes to the list of Equinix entities bound by this Policy to the relevant Data Protection Authorities in the EEA and Switzerland, via the competent Data Protection Authority with a brief explanation of the reasons justifying the update. Where a modification would possibly affect the level of protection offered by this Policy or significantly affect this Policy (i.e. changes to the binding character), it will be promptly communicated to the relevant Data Protection Authorities in the EEA and Switzerland, via the competent Data Protection Authority.

Where a new Equinix entity is established (whether as a result of a creation of entity, merger or acquisition), Equinix will ensure that this entity is bound by this Policy and abides by the principles set out in the Binding Corporate Rules and that transfers of Personal Data relating to European Data Subjects to this new entity are done only once this entity is effectively bound by and is compliant with this Policy.