Data Protection Policy

CONSTRUCTEL

CONNECTING THE WORLD OF TOMORROW

Índice

1. Scope and Purpose

This Internal Data Protection Policy ("**Data Protection Policy**") provides the principles for the Processing of Personal Data within Constructel Visabeira, S.A., herein referred to as "Constructel", and facilitates in compliance with Constructel's data protection obligations.

This Data Protection Policy applies to Constructel and its subsidiaries and applies to all Constructel employees and Processing of Personal Data within Constructel. It will be reviewed periodically and may be updated from time to time. Non-compliance with this Data Protection Policy by Constructel employees may lead to the application of disciplinary sanctions.

This Data Protection Policy may also refer to, and should be read in conjunction with, various Constructel policies relevant to the Processing of Personal Data including, but not limited to: the Information Security Policy, Employee Privacy Notice, Business Privacy Notice, Consumer/Customer Privacy Notice and Records of Processing Activities.

Constructel needs to gather and use certain information about individuals. These individuals may include, for example, Constructel's own employees, the employees of our customers and suppliers, business contacts, and other individual people the organization has a relationship with or may need to contact. This Data Protection Policy reflects and details Constructel's respect for the privacy of those individuals and its commitment to compliance with applicable data protection legislation.

This Data Protection Policy sets out a base standard for compliance. Where local applicable laws apply stricter standards, Constructel will seek to meet those standards. Where applicable, each country will adhere to any additional requirements or deviations from this Data Protection Policy as required by local applicable laws.

If you wish to discuss the contents of this Data Protection Policy or have any questions or queries regarding privacy or data protection within Constructel, please contact the Constructel Data Protection Officer ("DPO") at dpo@constructel.com.

2. Data Protection Laws

There are a number of data protection laws around the world that regulate the way Constructel uses Personal Data.

For example, where Constructel is established in the EEA or United Kingdom, those entities must meet the requirements of the EU GDPR and UK GDPR respectively, and other applicable local laws supporting the GDPR. Where applicable, the GDPR is underpinned by eight important principles. These are that Personal Data must be:

- Processed fairly and lawfully,
- Obtained only for specific, lawful purposes,
- Adequate, relevant and not excessive,
- Accurate and kept up to date,
- Not held for longer than necessary,
- Processed in accordance with the rights of Data Subjects,
- Protected in appropriate ways,
- Not transferred outside the European Economic Area ("EEA") unless that country or territory also ensures an adequate level of protection.

3. Responsibility

This Data Protection Policy is linked to the Constructel Information Security and Data Protection Notices, and is as such under the responsibility of the IT Department. The IT Department is responsible for ensuring that the Data Protection Policy is applied in all Business Units. The Data Protection Organization, through its Security and Privacy Commission ("SPI") as described herein, is responsible for the implementation of the Data Protection Policy. All Constructel employees are responsible for adhering to this Policy.

Constructel and every Business Unit acting as Controller shall be responsible for and be able to demonstrate compliance with this Data Protection Policy.

4. Definitions

The following definitions shall have the same meaning as the relevant definitions set out in the GDPR.

Business Unit

Business Unit shall mean all subsidiaries that Constructel either directly or indirectly controls more than 50% of the voting interest in.

Consent

Consent means any freely given, specific, informed and unambiguous indication of a Data Subject's wishes by which the Data Subject, by a statement or a clear affirmative action, signifies his/her agreement to the Processing of Personal Data relating to him/her.

Controller

The Controller means the natural or legal person, e.g. Constructel and/or a Business Unit, which alone or jointly with others determines the purpose and means of the Processing of Personal Data.

Data Subject

An identified or identifiable natural person who can be identified, directly or indirectly, 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 natural person. A Data Subject may for example be an employee or contractor of Constructel, a client or supplier representative, a person applying for a job at Constructel or subscribing to information by entering information on Constructel´s website or a representative from a business partner of Constructel.

EEA

The European Economic Area, meaning the EU member states together with the EFTA countries (Liechtenstein, Iceland and Norway).

GDPR

The GDPR shall mean the EU General Data Protection Regulation 2016/679.

Joint Controllers

Joint Controllers shall mean the situation where two or more Controllers jointly determine the purposes and means of the Processing.

Personal Data

Personal Data means any information relating to an identified or identifiable individual (the "Data Subject"). Personal Data includes all types of information that directly or indirectly may be linked to the Data Subject.

By way of examples, Personal Data may include:

- Names, dates of birth, SAP ID, passport details;
- Contact details such as addresses, e-mail addresses, telephone numbers, instant message identification and social media profiles;
- Indirect information such as IP address and laptop name;
- Expressions of opinions on living individuals;
- Location data;
- Information concerning salary and payment information;
- Client and supplier information (if linked to an individual).

Processing

Any operation or set of operations which is performed upon Personal Data or on sets of Personal Data, whether or not by automatic means, such as use, collection, recording, organization, structuring, alignment or combination, adaptation or alternation, retrieval, consultation, dissemination, storage and disclosure by transmission or otherwise making available, restriction, erasure or destruction.

The definition is technology-neutral and includes the Processing of Personal Data that is wholly or partially performed with the aid of computers or similar equipment that is capable of automatically Processing Personal Data. The definition also includes manual registers or filing systems if the Personal Data is included in, or is intended to form part of, a structured collection, making the Personal Data available for searching or compilation according to specific criteria.

Personal Data Breach

Personal Data Breach shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed such as:

- Indirect information, such as IP address and laptop name
- Expressions of opinions on living individuals
- Location data
- Information concerning salary and payment information
- Client and supplier information (if linked to an individual)

Processor

A natural or legal person, public authority, agency or other body, which Processes the Personal Data on behalf of a Controller, for example an outsourcing partner or service provider which Processes Personal

Data on behalf of a Business Unit.

Special categories of data (Sensitive Data)

Special categories of data are Personal Data revealing or concerning:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- genetic data,
- biometric data for the purpose of uniquely identifying a Data Subject,
- health,
- sex life or sexual orientation.

Third Country

Third Country, in the context of international transfers, shall mean any country outside the European Economic Area ("EEA") that has not been determined by the relevant supervisory or government authority of the country of export to have adequate data protection laws.

5. General staff guidelines

- Staff should only be able to access Personal Data covered by this Data Protection Policy if it is needed for their work.
- Data should not be shared informally. When access to large volumes of Personal Data or inherently private Personal Data is required, employees can request it from their managers.
- Constructel will provide training to all employees to help them understand their responsibilities when handling personal data, and provide an e-learning platform through its intranet, for them to access information on new training availability and related support material.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

- In particular, strong passwords must be used and they should never be shared.
- Personal Data should not be disclosed to unauthorized people, either within the company or externally.
- Personal Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their manager or the DPO if they are unsure about any aspect of data protection.

6. Key principles of the Data Protection Policy

Data Subjects' rights

Data Subjects (e.g. employees, contractors, individual customers and other third parties) whose Personal Data is being processed by Constructel entities that are subject to the GDPR benefit from the following rights:

Information regarding how their Personal Data is being used:

Data Subjects have a right to be informed about how Constructel will use and share their Personal Data. This explanation must be provided to individuals in a concise, transparent, intelligible, and easily accessible format. Privacy notices must be written in clear and plain language and must be provided free of charge.

Rights of access:

Under the right of access, Data Subjects have a right to:

- obtain confirmation of whether Constructel is Processing their Personal Data;
- access to their Personal Data; and
- information regarding how their Personal Data is being used by Constructel.

Every request from data subjects is handled by the DPO through a CRM platform and replied within the legal time frame. The requests for access and deletion of data are also processed through a ticket support, directed to the relevant parties to the data processing in case.

Further information about the procedure for handling Data Subject requests can be found in section 10 of this Data Protection Policy.

Right of rectification:

Data Subjects have a right to have any inaccurate or incomplete Personal Data rectified.

Right of erasure (in certain circumstances):

Data Subjects have a right to request that certain information held by Constructel is erased. This is also known as the right to be forgotten. This is not an absolute or blanket right to require all Personal Data to be deleted. For example, if information is required to exercise or defend legal claims, then it is not necessary for Constructel to delete the Personal Data.

Right to restrict Processing and blocking of data:

Data Subjects have a right to block the Processing of their Personal Data in certain circumstances. If a request to restrict Processing is made then it will be necessary for Constructel to determine whether the request should be upheld and whether procedures need to be put in place to restrict use of the relevant Personal Data.

Right to data portability:

In certain circumstances Data Subjects can request to receive a copy of their Personal Data in a commonly used electronic format. This right only applies to information that Data Subjects have provided to Constructel (for example by completing a form or providing information through a website).

Right to object to the Processing in certain circumstances (e.g. when Personal Data is used for marketing purposes):

Data Subjects have a general right to object to data Processing being carried out by Constructel in certain circumstances (e.g., if Constructel is using Personal Data for direct marketing purposes). Any Constructel employee that receives an objection to marketing must ensure that the relevant Data Subject is identified on the relevant system or record as having opted-out of marketing. In the event of any uncertainty, contact the Constructel DPO.

Rights in relation to automated decision making and profiling:

Data Subjects have a right not to be subject to a decision which is based on automated Processing where the decision will produce a legal effect or a similarly significant effect on them. If you are a Constructel employee and suspect that such Processing is taking place, seek advice from the Constructel DPO in relation to the steps that need to be taken to ensure that the automated decision making is carried out in a compliant way.

Information about Data Subjects' rights

Data Subjects who benefit from the rights set out in this Data Protection Policy can find more information about the exercise of their rights in the privacy notices for: Consumers, Businesses and Employees.

7. Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Department or Controller.

Physical data (i.e., printed documents)

When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it. Specifically:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left unattended where unauthorized people could see them, like a desk or on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

Further information on the security of physical data can also be found in our Security Policy (i.e., GVB_Critical Facilities Access Management Procedure) and Backup Policy (GV_Backup_Policy).

Electronic data

When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts. The following measures must be taken to protect electronic data:

- Data should be protected by strong passwords that are changed every 90 days (at a minimum) and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service.
- Servers containing Personal Data should be sited in a secure location, away from general office space.

- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.
- All systems should be updated centrally and regularly with latest anti-virus and firewalls

8. Data use

Personal Data is of no value to Constructel unless the business can make use of it. However, it is when Personal Data is accessed and used that it can be at the greatest risk of loss, corruption or theft. Therefore:

- When working with Personal Data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal Data should not be shared informally. In particular, large volumes of Personal Data or inherently private Personal Data (or other datasets of Personal Data that have the potential to create risks for individuals if intercepted) should never be sent by unencrypted email.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorized external contacts.
- Personal Data should never be transferred outside of the European Economic Area without prior consultation with the Data Protection Office.
- Employees should not save copies of Personal Data to their local drive on their own computers. Instead, employees should always access and update the central copy of any data.

9. Data accuracy

The law requires Constructel and its employees to take reasonable steps to ensure data is kept accurate and up to date. Such steps should include but are not limited to:

- Where possible, holding Personal Data in as few places as necessary. Staff should not create any duplicates of Personal Data when not required to do so by a compelling reason.

- Staff should take every opportunity to ensure Personal Data of third parties is kept up to date. For instance, this can be done by confirming whether the customer's personal details have changed during a call.
- Customer-facing employees should be able to update customer Personal Data held by Constructel. Individuals should also be able to request updates to their personal details easily, for instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a number held for a customer has been determined to be incorrect, it should be removed from the database.
- It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

10. General privacy principles observed by Constructel

The following general principles are based on the principles of the GDPR and applicable EU/EEA data protection law, where it applies. Further details may be set out in data privacy and information security global procedures applicable to all Business Units. Any inquiries concerning the general principles should be addressed to the Group or Local Privacy Officer.

Lawfulness, fairness and transparency

Personal Data shall be processed fairly, lawfully, in a transparent manner and pursuant to the principles stipulated in this Data Protection Policy (and any other relevant policies of Constructel).

Purpose limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Data minimization, accuracy and storage limitation

Personal Data shall be:

(a) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected and/or further Processed ("data minimization");

(b) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate, having regard to the purposes for which they were collected or for which they are further Processed, are erased or rectified without delay ("accuracy"); and

(c) Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further Processed ("storage limitation").

Lawful Processing of Personal Data

Personal Data should be processed only where one or more of the following legal bases applies:

(a) the Data Subject has given Consent to the Processing of his or her Personal Data for one or more specific purposes;
(b) Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
(c) Processing is necessary for compliance with a legal obligation to which the Controller is subject;
(d) Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller; or
(f) Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data.

Processing of Sensitive Data

It is generally prohibited to Process Sensitive Data, meaning Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or to Process genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, sex life or sexual orientation. Sensitive Data may only be processed if:

(a) The Data Subject has given explicit Consent to the Processing of those data for one or more specified purposes, except where the local laws applicable to the Business Unit provide that the prohibition above may not be lifted by the Data Subject.
(b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorized by local law or a collective agreement pursuant to local law providing for appropriate safeguards for the

fundamental rights and the interests of the Data Subject;

(c) Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving Consent;

(d) Processing relates to data which are manifestly made public by the Data Subject;

(e) Processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;

(f) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health, social care, treatment or the management of health or social care systems and services on the basis of local law or pursuant to a contract with a health professional that is subject to the obligation of professional secrecy or another person subject to an equivalent obligation of secrecy; or

(g) Processing is allowed according to national rules other than (a) to (f) above, and the national rules have been established in accordance with the GDPR.

Conditions for Consent

If Consent is allowed or required under the GDPR for the Processing of Personal Data or Processing of Sensitive Data, the following conditions apply:

(a) Constructel must be able to demonstrate that it has obtained the Data Subject's Consent to the Processing of his/her Personal Data in an informed, voluntary and specific manner;

(b) Constructel must ensure the following in relation to any Consent it obtains:

i) If the Data Subject's Consent is given in the context of a written declaration which also concerns other matters, the request for Consent shall, where applicable law so requires, be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible format, using clear and plain language; and

ii) Consent is only to be used when it is likely to be valid as a legal basis for the Processing. With regard to employment relationships, Consent should therefore not be used as a legal basis, unless it is clear that it is freely given. This will typically be when the Data Subjects voluntarily participate in a survey or events arranged by Constructel or register for an internal newsletter from Constructel.

(c) The Data Subject may withdraw his/her Consent at any time and the Data Subject shall, where applicable law so requires, be informed of his or her right to withdraw the Consent. The withdrawal of Consent shall not affect the lawfulness of the Processing based on such Consent before its withdrawal. It shall be as easy to withdraw as to give Consent.

Procedure for handling Data Subject's requests

Prior to fulfilling a Data Subject's request to exercise a data protection right, the Controller should request proof of the individual's identity. Once their identity has been verified, the Controller must not delay in responding to the request. The Controller may seek further details from the Data Subject regarding the request (e.g., if the Data Subject is aware of the circumstances in which the Controller obtained the Personal Data or the systems the relevant Personal Data is likely to be stored on).

When a request has been made by electronic means, the response shall be provided in the same manner where possible (provided the medium is secure), unless otherwise requested by the Data Subject. The request shall be responded to without undue delay and in any event within one month of receipt of the request. This period may be extended by two more months where necessary, considering the complexity of the request. In such cases, the Data Subject shall be informed of any such extension within one month from receipt of the request, together with the reasons for the delay.

In the case of an objection, the relevant Data Privacy Officer shall respond by confirming whether or not the particular Processing will be stopped. If the Processing is not stopped, the communication must be accompanied with the reasons for continuing the Processing.

Confidentiality of Processing

Any person acting under the authority of the Controller or of the Processor, including the Processor himself, who has access to Personal Data must not Process this except on instructions from the Controller, unless he/she is required to do so by law.

Joint Controllers

In situations where two or more Controllers jointly determine the purposes and means of the Processing, they shall be considered Joint Controllers. Such situations may arise when two Business Units together determine the purposes and means of the Processing, which may be the case e.g. in joint research projects.

Whether two or more Controllers are Joint Controllers must be assessed on a case-by-case basis and depends on whether there is any joint determination in relation to the purposes and means of the Processing. In the cases of Joint Controllers, they shall determine in a transparent manner their respective responsibilities for compliance with applicable EU/EEA data protection law, in particular as regards the information requirements and the Data Subjects rights.

The parties' respective responsibilities shall be described in an arrangement between the parties, in particular as regards the exercising of the rights of the Data Subject and their respective duties to provide the information. In addition, the arrangement shall typically include:

- description of the Processing and data flow map;
- the parties' responsibilities with regard to data protection compliance;
- disclosure of data and confidentiality;
- technological and organizational security measures and conduction of risk assessment;
- use of subcontractors;
- data transfers to Third Countries;
- deletion and return of data;
- applicability of internal procedures;
- liability.

The essence of the arrangement shall be made available to the Data Subject and shall duly reflect the parties' respective roles and the relationships of the Joint Controllers towards the Data Subjects.

Use of data Processors

When Constructel is subject to the GDPR and contracts with service providers for the delivery of services involving Processing of Personal Data on behalf of Constructel, only Processors providing sufficient guarantees to implement technical and organizational measures in such a manner that the Processing will meet the GDPR requirements shall be chosen.

The Processing by a Processor shall be governed by a contract (a Data Processing Agreement) that, as a minimum, sets out the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of the Data Subjects and the obligations and rights of the Controller. The contract shall stipulate, in particular that the Processor:

(a) Processes the Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a Third Country or an international organization, unless required to do so by national law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required by law related to the security of Processing;

(d) respects the conditions referred to below related to engagement of another Processor;

(e) taking into account the nature of the Processing, assists the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights under applicable EU/EEA data protection law;

(f) assists the Controller in ensuring compliance with the legal obligations related to security of Processing and consultation with the Supervisory Authorities taking into account the nature of Processing and the information available to the Processor;

(g) at the choice of the Controller, deletes or returns all the Personal Data to the Controller after the end of the provision of services relating to Processing, and deletes existing copies unless applicable law requires storage of the Personal Data;

(h) makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Data Protection Policy and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. The Processor shall not engage another Processor without prior specific or general written authorization of the Controller. In the case of general written authorization, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other Processors, thereby giving the Controller the opportunity to object to such changes.

Data protection by design and by default

The Controller shall, both when determining the means for Processing and at the time of the Processing, implement appropriate technical and organizational measures, which are designed to implement data protection principles, such as data minimization, in an effective manner, in

order to integrate the necessary safeguards into the Processing for protecting Data Subjects' rights.

The Controller shall implement appropriate technical and organizational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are processed.

This obligation applies to the amount of Personal Data collected, the extent of their Processing, the period of their storage and their accessibility. These measures shall particularly ensure that by default, Personal Data are not made accessible without intervention to an indefinite number of persons. Please refer to the applicable Constructel procedure for applying these principles.

Personal Data Breach Notification

If a Personal Data Breach has occurred or is suspected to have occurred, the person who has become aware of or suspects the Personal Data Breach, shall immediately notify the respective manager or the DPO, who will forward the incident to the Group's Security and Privacy Commission (SPI).

A Personal Data Breach occurs for example if the Controller's data systems are hacked, Personal Data is accidentally or intentionally sent to the wrong recipient, Personal Data is left in a place where unauthorized personnel can access the data, data theft and other kinds of data leaks.

Constructel has established a procedure for Controlling and Processing of Personal Data which shall be followed when handling Personal Data Breaches. Please consult this procedure (GVB_SGSI.PL.14.03 - Incident Management) for details and timelines for determining when notification to the competent Data Protection Authority and the concerned Data Subjects is required.

Constructel shall document any Personal Data Breaches, comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken. That documentation shall be made available to the competent Data Protection Authority upon request.

11. Transfers

Transfer of Personal Data to Controllers and Processors that are members of the group (internal transfer)

Transfer from Controller to Controller

Transfer of Personal Data between Controllers may take place, provided that:

(a) it is not incompatible with the purpose for which the Personal Data were collected,

(b) it is in accordance with the principle of minimization, accuracy and storage limitation,

(c) the criteria for making Data Processing lawful is fulfilled (e.g. a lawful basis, such as legitimate interests, has been identified),

(d) if applicable, information is given to the Data Subject (e.g. in privacy notices),

(e) appropriate security measures protect the data during transfer and further Processing by the receiving Controller, and

(f) if the transfer is from a Controller established within the EEA to a Controller in a Third Country, the requirements immediately below are met.

Applicable local law may have additional requirements and should always be considered before making such transfers.

Transfer to external Processors established outside the EEA

Transfer of Personal Data from a Controller established within the EEA to a Processor in a Third Country is prohibited, except when the conditions are fulfilled and one of the legal bases in Articles 45, 46, 47 or 49 of the GDPR are met, including (by way of examples):

(a) The transfer is governed by approved Binding Corporate Rules or a similar transfer mechanism that provides appropriate safeguards under applicable law;

(b) Controller and the Processor have provided appropriate safeguards by entering into EU Standard Contractual Clauses (model contract);

(c) an approved code of conduct or an approved certification mechanism pursuant to Article 46(1) (e) and (f) of the GDPR are provided for.

12. Changes to Internal Data Protection Policy

A full copy of this Internal Data Protection Policy can be obtained, digitally, from Constructel's website (www.constructelvisabeira.com), and a physical copy from the Human Resources department.

For the effectiveness of this document no significant changes are foreseen, however, in matters of detail, Constructel reserves the right to update this Internal Data Protection Policy at any time, with all changes deemed effective as of the date of posting. We will notify all of our employees and other participants of future material changes.

Related Documents

Doc ID	Description	Owner
GVB_SGSI.PL.01.01	General Information Security Policy	Information Security Committee
GVB_SGSI.PR.03.02	Security and Privacy Commission	Information Security Committee
GVB_Regulatory Standard - Use of IT Resources_V7.0	Employees use of IT Resources	Information Security Committee
GVB_SGSI.PL.05.01	Password Policy	Information Security Committee
GVB_SGSI.PR.12.01	Password Delivery - Annex A	Information Security Committee
GVB_SGSI.PL.06.01	Clean Desk and Clean Screen Policy	Information Security Committee
GVB_SGSI.NR.03.01	Use of e-Mail	Information Security Committee
GVB_SGSI.NR.04.01	Internet Access	Information Security Committee
GBV_SGSI.IM.02.01	Remote Access Responsibility Term	Information Security Committee
GV_Backup_Policy_1.1	Backup policy	IT Department
GVB_Critical Facilities Access Management Procedure_v5.0	Control of access to critical facility and data centers	IT Department
GVB_SGSI.IM.05.00	Delivery and Return of Assets	Information Security Committee

Document:	Data Protection Policy
Version:	1.0
Date:	2022, October 27