BRINK'S EUROPEAN DATA PROTECTION POLICY

TABLE OF CONTENTS

This European Data Protection Policy is intended to supplement Brink's Global Data Protection Policy in light of the specific requirements of the General Data Protection Regulation (EU) 2016/679 ("GDPR").

In case of conflict between Brink's Global Data Protection Policy and the European Data Protection Policy, the European Data Protection Policy will prevail for any of Brink's Personal Data Processing that is subject to GDPR.

A.
PURPOSE

As stated in the Brink's Code of Ethics, The Brink's Company, including its affiliates and subsidiaries, is committed to protecting the privacy and security of its customers, suppliers, employees, workers and other third parties.

This European Data Protection Policy exists to affirm Brink's commitment to comply with European privacy standards in terms of the collection and Processing of Personal Data, and to set forth how Brink's protects such data.

Capitalized terms or acronyms used in this Policy have the meanings set out in the "Terms/Roles and Definitions" page.

BELGIUM

B.
POLICY STATEMENT

In the context of its business activities, including the provision of products or services or employment of Brink's Personnel, Brink's may Process, be exposed to or come into possession of Personal Data.

As the Data Controller of all Personal Data relating to Brink's Personnel and Personal Data used for commercial purposes, Brink's commits to restrict and monitor access to Personal Data, train employees in applicable privacy and security measures, maintain established procedures for reporting Personal Data Breaches, and establish data protection practices as may be practical and/or required under the circumstances.

All lines of business, Brink's Entities, and Brink's Personnel are responsible for ensuring all Personal Data is obtained and/or Processed in compliance with this European Data Protection Policy and will implement appropriate practices, processes, controls, and attend training to ensure compliance.

C.
SCOPE

This European Data Protection Policy applies to all lines of Brink's business and Brink's Entities operating in the European Economic Area and the United Kingdom ("Europe"). It covers all Personal Data Processed by those Brink's Entities, regardless of the media in which the data is maintained, and may relate to prospective, past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subjects.

This European Data Protection Policy is intended to supplement Brink's Global Data Protection Policy in light of the specific requirements of the General Data Protection Regulation (EU) 2016/679 ("GDPR"). In case of conflict between Brink's Global Data Protection Policy and the European Data Protection Policy, the European Data Protection Policy will prevail for any of Brink's Personal Data Processing that is subject to GDPR.

D.
COMPLIANCE

All Brink's Personnel in Europe must read, understand, and comply with this European Data Protection Policy when Processing Personal Data on Brink's behalf. This European Data Protection Policy sets out what is expected in order for Brink's to comply with applicable law.

Compliance with this European Data Protection Policy and all Implementing Documentation is mandatory.

Any breach of this European Data Protection Policy may result in disciplinary action for Brink's Personnel in accordance with applicable law and in substantial financial penalties for Brink's (e.g., GDPR sets forth fines up to EUR 20 million or 4% of annual turnover, whichever is higher).

GREECE

E.
TERMS/ROLES & DEFINITIONS

3rd Party Mechanism: allows EU individuals to submit certain residual claims to arbitration to determine whether a Privacy Shield organization violated its obligations under the Privacy Shield principles as to that EU individual, and whether any such violation remains fully or partially unremedied.

Automated Decision-Making (ADM): when a decision is made which is based solely on automated Processing, including Profiling, which produces legal effects or significantly affects an individual.

Profiling: any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyze or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Brink's Entity: The Brink's Company or any of its subsidiaries.

Brink's Personnel: all Brink's employees, contractors, directors and members.

Consent: any freely given, specific, informed and unambiguous indication of an individual's wishes by which he or she, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to him or her.

Data Controller: the person or organization that determines why and how to Process Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data Processing activity.

Data Protection Officer (DPO): the person or team with responsibility for monitoring Brink's data protection compliance and formally appointed as such.

Data Subject: an identified or identifiable individual about whom we Process Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

EEA: the 27 countries in the EU, and Iceland, Liechtenstein and Norway.

EU Standard Contractual Clauses: the European Commission's standard data protection clauses for the Transfer of Personal Data to third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR.

Explicit Consent: consent which requires a clear and specific consent statement (that is, not just an action).

GDPR: the General Data Protection Regulation (EU) 2016/679.

Implementing Documentation: Brink's policies, operating procedures, processes or guidelines related to this Policy and designed to protect Personal Data.

JAMS: alternative dispute resolution (ADR) provider that provides Privacy Shield Annex I services pursuant to EU-U.S. and/or Swiss U.S. Privacy Shield program.

Personal Data: any information (1) relating to an identified or identifiable individual or (2) that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household. This includes information relating to an individual that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access, in particular identifiers such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that Data Subject. Personal Data excludes anonymous data or data from which the identity of an individual has been permanently removed.

Personal Data Breach: any actual or reasonably suspected unauthorized or accidental access to or loss, use, alteration, destruction, acquisition, or disclosure of, Personal Data transmitted, stored or otherwise Processed by Brink's or its service providers.

Privacy by Design: integrating Personal Data Processing procedures in the technology when created so as to ensure data privacy compliance.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when Brink's collects Personal Data about them.

Processing or Process: any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission or transfer to third parties, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Pseudonymization or Pseudonymized: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: Personal Data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms of the Data Subject, e.g., data revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

Transfer: any operation or set of operations which support the communication, copy or movement of Personal Data by using a network or any other medium, to the extent that such Personal Data is intended to be Processed by the third party who receives it. Remote access to Personal Data is an example of a Transfer.

IRELAND

F.
DATA PROTECTION OFFICER

Brink's has designated a Data Protection Officer (DPO) on May 25, 2018 as per article 37 of GDPR.

The DPO is responsible for overseeing this European Data Protection Policy and, as applicable, developing Implementing Documentation. Contact information for the DPO is attached in Appendix A.

For the avoidance of doubt, the overall responsibility of complying with this European Data Protection Policy lies with Brink's and not with the DPO (see Accountability section below).

Please contact the DPO or the Legal Department with any questions about this European Data Protection Policy or the GDPR or with any concerns that this Policy is not being or has not been followed. In particular, contact the DPO:

- If you are unsure of the lawful basis which you are relying on to Process Personal Data (including the legitimate interests used by Brink's);
- If you need to rely on Consent and/or need to capture Explicit Consent;
- If you need to draft a Privacy Notice;
- If you are unsure about the retention period for the Personal Data being Processed;
- If you are unsure about what security or other measures you need to implement to protect Personal Data;
- If there has been a Personal Data Breach;
- If you are unsure on what basis to use for a Transfer of Personal Data outside the EEA or the United Kingdom, as applicable;
- If you need any assistance dealing with any rights invoked by a Data Subject;
- Whenever you are engaging in a new, or change in an existing, Processing activity which is likely to require a DPIA or you are planning to use Personal Data for purposes other than that for which it was collected;
- If you plan to undertake any activities involving Profiling or Automated Decision-making;
- If you need help complying with applicable privacy laws when carrying out direct marketing activities; or
- If you need help with contracts or other areas in relation to sharing Personal Data with third parties (including our vendors).

FRANCE

ESTONIA

G.
DATA PROTECTION PRINCIPLES

Brink's adheres to the European data protection principles which require Personal Data to be:

- Processed lawfully, fairly, and in a transparent manner (Lawfulness, Fairness, and Transparency);
- Collected only for specified, explicit, and legitimate purposes and not further Processed in a manner that is incompatible with those purposes (Purpose Limitation);
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimization);
- Accurate and where necessary kept up to date (Accuracy);
- Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);
- Processed in a manner which ensures its security using appropriate technical and organizational measures to protect against unauthorized or unlawful Processing and against accidental loss, destruction, or damage (Security, Integrity, and Confidentiality);
- Not transferred to a third country without appropriate safeguards being in place (Transfer Limitation); and
- Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

Brink's is responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

G.1.
LAWFULNESS, FAIRNESS, AND TRANSPARENCY

Personal Data shall be collected and Processed lawfully and in a fair and transparent manner.

Lawful Processing

Any Processing carried out by Brink's as a Data Controller must have a legal basis under applicable data protection law, which include:

- the Data Subject has given his or her Consent to the Processing of his or her Personal data;
- the Processing is necessary for the performance of a contract with the Data Subject;
- the Processing is necessary to meet Brink's legal obligations;
- the Processing is necessary to protect Data Subject's vital interests; or
- the Processing is necessary to pursue Brink's legitimate interests where those interests are not overridden by the Data Subjects' interests, rights and freedoms. The purposes for which we Process Personal Data on this basis need to be set out in applicable Privacy Notices.

POLAND

Fair and Transparent Processing

Personal Data shall not be collected or obtained by deception or without the Data Subjects' knowledge.

When acting as a Data Controller, Brink's will provide detailed, specific information to Data Subjects depending on whether the Personal Data was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever Brink's collects Personal Data directly from Data Subjects, including for human resources or employment purposes, the Data Subject must be provided with a Privacy Notice containing all elements listed in Article 13 of the GDPR, including:

- the identity of the Data Controller and DPO,
- how and why Brink's will use, Process, disclose, protect and retain that Personal Data, and
- the rights available to the Data Subject in relation to his or her Personal Data and how the Data Subject may exercise these rights.

Such Privacy Notice must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), Brink's must provide the Data Subject with all the information required under Article 14 of the GDPR as soon as possible after collecting/receiving the data and at the latest within one month.

Notwithstanding the foregoing, the Privacy Notice must be provided:

- if the Personal Data is used to communicate with the Data Subject, at the latest at the time of the first communication; and
- if the Personal Data is disclosed to another recipient, at the latest at the time of the first disclosure.

Brink's must also check that the Personal Data was collected by the third party on a basis which contemplates proposed Processing of that Personal Data.

LITHUANIA

NETHERLANDS

G.2.
CONSENT

Brink's must only Process Personal Data on the basis of one or more of the lawful bases set out in the above section, which include Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing.

Consent requires affirmative action so silence, pre-ticked boxes, or inactivity are insufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be able to withdraw Consent to Processing easily at any time and withdrawal must be promptly honored. Consent may need to be sought again if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Explicit Consent is usually required when relying on Consent for Processing Sensitive Personal Data, for Automated Decision- Making and for cross border data Transfers. Brink's will rely on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Personal Data unless required. Where Explicit Consent is required, Brink's will issue a Privacy Notice together with a Consent request to the Data Subject to capture Explicit Consent. Brink's must evidence Consent captured and keep records of all Consents so that Brink's can demonstrate compliance with Consent requirements.

G.3.
PURPOSE LIMITATION

Personal Data shall be collected for one or more specified, explicit and legitimate purposes. It shall not be further Processed in any manner incompatible with those purposes. Personal Data cannot be used for new, different or incompatible purposes from those that are disclosed when Personal Data was first obtained unless Data Subjects are informed of the new purposes and they have consented where necessary.

G.4.
DATA MINIMIZATION

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. Brink's Personnel may only Process Personal Data when performing job duties requires it. Brink's Personnel may only collect Personal Data required for their job duties and may not collect excessive data.

Brink's shall ensure that any Personal Data collected is adequate and relevant for the intended purposes and that Personal Data is deleted or anonymized when it is no longer needed for specified purposes, in accordance with Brink's data retention guidelines.

G.5.
ACCURACY

Personal Data shall be recorded as accurately as possible and, where necessary, updated to ensure it fulfills the legitimate purpose(s) for which it is Processed.

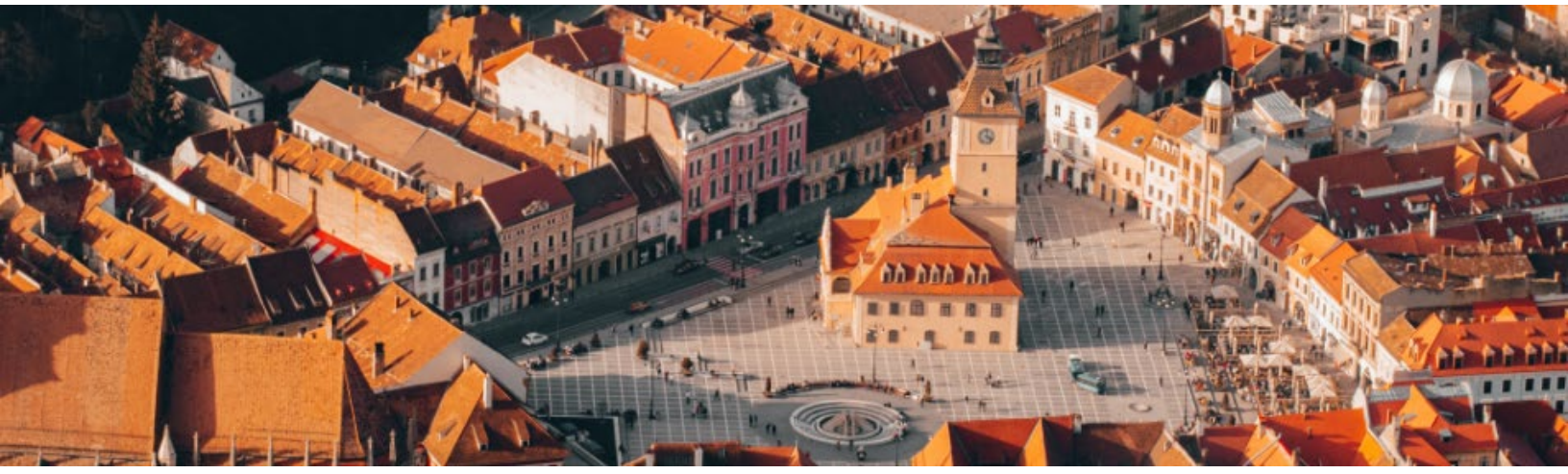
The accuracy of any Personal Data shall be checked at the point of collection and at regular intervals afterwards and all reasonable steps shall be taken to destroy or amend inaccurate or out-of-date Personal Data without delay.

G.6.
STORAGE LIMITATION

Personal Data shall not be kept in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which it was originally collected including for the purpose of satisfying any legal, accounting or reporting requirements.

Brink's will maintain retention policies and procedures to ensure Personal Data is deleted in accordance to applicable retention requirements. Brink's will take all reasonable steps to destroy or erase from systems all Personal Data that is no longer required in accordance with all Brink's applicable records retention schedules and policies and with applicable local laws. This includes requiring third parties to delete such data where applicable. Brink's will ensure that Data Subjects are informed of the period for which their Personal Data is stored or how that period is determined in any applicable Privacy Notice.

ROMANIA



UNITED KINGDOM

G.7.
TRANSFER LIMITATION

Brink's commits to only Transfer Personal Data outside the EEA or the UK, as applicable, if one of the following conditions applies:

- the European Commission has issued a decision confirming that the country to which Personal Data is transferred ensures an adequate level of protection for the Data Subjects' rights and freedoms on the basis of Article 45 of GDPR;
- appropriate safeguards are in place in accordance with Article 46 of the GDPR, including, but not limited to, binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
- the Data Subject has provided Explicit Consent to the proposed Transfer after being informed of any potential risks; or
- where the Transfer is occasional and not repetitive, that Transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

US Brink's Entities are self-certified under the EU-U.S. Data Privacy Framework, including its UK extension, and the Swiss-U.S. Data Privacy Framework, and adhere to the principles of these Data Privacy Frameworks.

These principles are available through this link:
https://www.dataprivacyframework.gov/s/key-requirements

Complaints under the Data Privacy Frameworks can be filed through this link:
https://www.jamsadr.com/submit/

G.8.
DATA SUBJECT'S RIGHTS AND REQUESTS

Data Subjects have rights regarding how Brink's Processes their Personal Data.

These include rights to:

- withdraw Consent to Processing at any time;
- receive certain information about Processing activities;
- request access to their Personal Data;
- prevent use of their Personal Data for direct marketing purposes;
- ask to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- restrict Processing in specific circumstances;
- challenge Processing which has been justified on the basis of legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- obtain human intervention, express their point of view and contest decisions based solely on ADM;
- prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the 3rd Party Mechanism: Brink's has designated JAMS as its U.S.-based third-party dispute resolution provider for non-employee data; JAMS can be contacted through their website, jamsadr.com; and
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

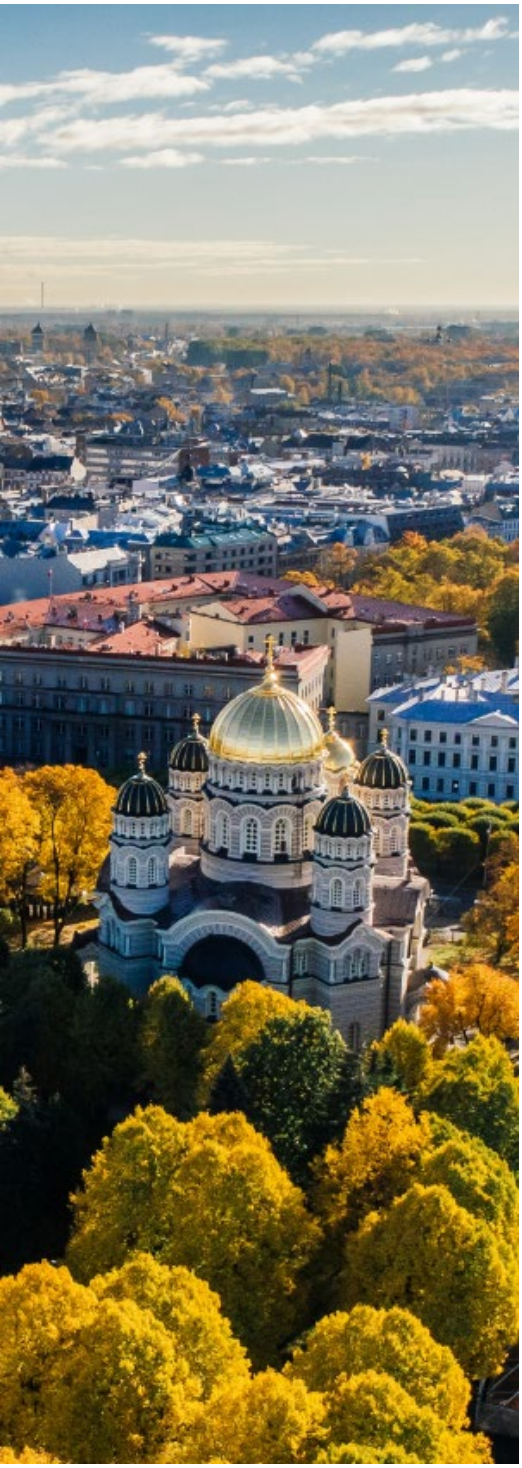
Brink's must verify the identity of an individual requesting data under any of the rights listed above. Brink's Personnel shall be cautious not to allow third parties to persuade them into disclosing Personal Data without proper authorization. Any employee/job applicant Data Subject requests received must be forwarded to the HR Representative / Department Head immediately upon receipt. Any customer Data Subject requests received must be forwarded to Business Representative / Customer Support immediately upon receipt.

The HR and Business Representatives will promptly inform the DPO (or designee) of any Data Subject requests and of the action undertaken to handle it.

Brink's must verify the identity of an individual requesting data under any of the rights listed above. Brink's Personnel shall be cautious not to allow third parties to persuade them into disclosing Personal Data without proper authorization. Any employee/job applicant Data Subject requests received must be forwarded to the HR Representative / Department Head immediately upon receipt. Any customer Data Subject requests received must be forwarded to Business Representative / Customer Support immediately upon receipt.

The HR and Business Representatives will promptly inform the DPO (or designee) of any Data Subject requests and of the action undertaken to handle it.

ITALY



LATVIA

G.9.
PROTECTING PERSONAL DATA

Personal Data must be safeguarded by appropriate technical and organizational safeguards designed to protect against Personal Data Breaches.

Brink's maintains safeguards appropriate to our size, scope and business, our available resources, the amount and sensitivity of Personal Data that we Process on our own behalf or on behalf of others and the identified risks to our systems and data. This includes without limitation the use of encryption and Pseudonymization, where applicable.

Brink's Information Security and Compliance team will regularly evaluate and test the effectiveness of those safeguards to help ensure security of our Processing of Personal Data.

Brink's Personnel are responsible for protecting the Personal Data held by Brink's and must ensure compliance with such safeguards. In particular, Brink's Personnel must exercise particular care in protecting Sensitive Personal Data from loss and unauthorized access, use or disclosure.

All procedures and technologies are in place to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data may only be transferred to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested, including by entering into a data processing agreement pursuant to Article 28 of the GDPR.

Brink's Personnel must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorized to use the Personal Data can access it;
- Integrity means that Personal Data is accurate and suitable for the purpose for which it is Processed;
- Availability means that authorized users are able to access the Personal Data when they need it for authorized purposes.

G.10.
REPORTING A PERSONAL DATA BREACH

Brink's has put in place procedures to address Personal Data Breaches and will notify Data Subjects and/or applicable regulators where legally required or otherwise appropriate.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact Information Security at:

ITSecurityTeam@brinksinc.com

All evidence relating to the Personal Data Breach must be preserved.

CZECH REPUBLIC

H.
ACCOUNTABILITY

Brink's will maintain appropriate technical and organizational measures in an effective manner to ensure compliance with data protection principles. Brink's is responsible for, and must be able to demonstrate compliance with the data protection principles, including by:

- appointing a suitably qualified local DPO where applicable and Global DPO responsible for monitoring GDPR compliance;
- implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
- integrating data protection into internal documents including this European Data Protection Policy, Implementing Documentation or Privacy Notices;
- regularly training Brink's Personnel in GDPR, this European Data Protection Policy, Implementing Documentation and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. Brink's must maintain a record of training attendance by Brink's Personnel; and
- regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

LUXEMBOURG

GERMANY

H.1.
RECORD KEEPING

Brink's will maintain accurate corporate records with respect to its Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with the Brink's record retention guidelines.

Records should include, at a minimum:

- the name and contact details of the Data Controller and the DPO;
- clear descriptions of the Personal Data types,
- Data Subject types;
- Processing activities;
- Processing purposes;
- third-party recipients of the Personal Data;
- Personal Data storage locations;
- Personal Data transfers;
- the Personal Data retention period(s);
- documented data flows;
- and a description of the security measures in place.

H.2.
TRAINING AND AUDIT

Brink's will provide training for all Brink's Personnel to enable them to comply with this European Data Protection Policy. Brink's will also regularly test systems and processes to assess compliance and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

H.3.
PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Brink's will comply with the principles of Privacy by Design and by Default when Processing Personal Data, in particular by implementing appropriate technical and organizational measures (like Pseudonymization) in an effective manner, to ensure compliance with data protection principles.

All programs/systems/processes that Process Personal Data must be assessed for Privacy by Design by taking into account the following:

- the state of the art;
- the cost of implementation;
- the nature, scope, context and purposes of Processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

DPIAs shall be conducted in respect to high-risk Processing and when implementing major system or business change programs involving the Processing of Personal Data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Profiling and ADM;
- large scale Processing of Sensitive Personal Data; and
- large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- a description of the Processing, its purposes and the legitimate interests pursued if appropriate;
- an assessment of the necessity and proportionality of the Processing in relation to its purpose;
- an assessment of the risk to Data Subjects; and
- the risk mitigation measures in place and demonstration of compliance.

DPIA findings must be discussed with the DPO.

GREECE

H.4. PROFILING AND AUTOMATED DECISION-MAKING

Automated Decision Making is prohibited when a decision has a legal or similar significant effect on an individual unless:

- the Data Subject's Explicit Consent has been obtained;
- the Processing is authorized by law; or
- the Processing is necessary for the performance of or entering into a contract with the Data Subject.

If Sensitive Personal Data is being Processed, then second and third grounds above will not be allowed but such Sensitive Personal Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on automated Processing (including Profiling), then Data Subjects must be informed of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests. Data Subject must also be informed of the logic involved in the decision making or Profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Profiling or ADM activities are undertaken.

H.5. DIRECT MARKETING

Brink's must obtain Data Subjects' Consent prior to sending electronic direct marketing communications. The limited exception for existing customers known as "soft opt in" allows Brink's to send marketing texts or emails if:

- Brink's has obtained the customer's contact details in the course of a sale to that person;
- Brink's is marketing similar products or services; and
- Brink's gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information. A Data Subject's objection to direct marketing must be promptly honored. Brink's may retain just enough information to ensure that marketing preferences are respected in the future.

CYPRUS

FRANCE

H.6.
SHARING PERSONAL DATA

Brink's Personnel may only share Personal Data held by Brink's with another employee, agent or representative of Brink's affiliates if the recipient has a job-related need to know the information and the Transfer complies with any applicable cross-border transfer restrictions.

Personal Data we hold may be shared with third parties, such as our service providers if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the Transfer complies with any applicable cross border transfer restrictions; and
- a fully executed written contract - or amendment to an already existing contract - that contains
- GDPR approved third party clauses has been obtained.

I.
ANNUAL REVIEW

Brink's reserves the right to change this European Data Protection Policy at any time. Brink's Global DPO will consistently monitor and periodically assess this European Data Protection Policy to ensure it complies with the GDPR.

Notwithstanding the foregoing, this European Data Protection Policy will be formally reviewed and updated as appropriate at least once annually by Brink's Global DPO and Brink's Global Privacy Counsel. In the event the European Data Protection Policy requires changes due to regulatory or other requirements, then the European Data Protection Policy will be promptly amended to reflect such changes.

PORTUGAL

APPENDIX
Data Protection Officer

Brink's Global DPO under GDPR is Guillaume Nonain : **dpo_gdpr@brinksinc.com**.

Brink's local DPOs (when one has been appointed at country level) contact details are available through the Global DPO or the Global Legal Intranet and its Data Protection section (see p. 21).