Table of Contents

1.0 Introduction

1.1 Purpose

As stated in The Brink's Company Code of Ethics, The Brink's Company, including all of its subsidiaries[1] ("Brink's", "we", "our", "us", "the Company") is committed to protecting the privacy and security of its customers, suppliers, employees, workers and other third parties. This Privacy Policy exists to affirm Brink's commitment to comply with the highest standards in data privacy requirements, in terms of the collection and processing of personal data, and how Brink's protects such data.

In keeping with Brink's above commitment to the privacy of customers, employees and third parties, Brink's is self-certified under the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework (collectively the "Privacy Shield") as agreed to and set forth by the U.S. Federal Trade Commission, the U.S. Department of Transportation and the European Union. To learn more about the Privacy Shield and to obtain a copy of the Privacy Shield Principles, please visit this page. To obtain a copy of the Privacy Shield List, please visit this page.

1.2 Scope

This Privacy Policy applies to all Company Personnel ("you", "your"). It covers all Personal Data Processed by Brink's regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

Even though this Privacy Policy was designed to make Brink's policy in line with the General Data Protection Regulation (*EU 2016/679)* ("GDPR"), which applies to companies based in the European Union as well as companies elsewhere which provide or offer goods or services, and which process data from or about people in the EU, it is meant to apply globally but does not override any applicable data privacy laws and regulations in countries where the Company operates. Certain countries may also have localized variances to this Privacy Policy which may be displayed on their websites or available upon request to the local DPO, Legal or Human Resources Representative.

1.3 Compliance

All Company Personnel must read, understand, and comply with this Privacy Policy when Processing Personal Data on Brink's behalf. This Privacy Policy sets out what is expected in order for the Company to comply with applicable law. Compliance with this Privacy Policy and all such Related Policies and Privacy Guidelines is mandatory. Any breach of this Privacy Policy may result in disciplinary action for the individuals 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).

[1] A list of Brink's U.S. subsidiaries to which this Privacy Policy applies can be found in Appendix A.

1.5 Terms/Roles and 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 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.

Automated Processing: 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. Profiling is an example of Automated Processing.

Company: The Brink's Company, including all of its subsidiaries.

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

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organization that determines when, why and how to process Personal Data.

Data Subject: a living, identified or identifiable individual natural person about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their 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.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

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

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

International Centre for Dispute Resolution (ICDR): the international division of the American Arbitration Association (AAA) and provides Privacy Shield Annex I services pursuant to EU-U.S. and/or Swiss-U.S. Privacy Shield program.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject 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 that has had the identity of an individual permanently removed.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organizational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorized access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

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 the Company collects information 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.

Pseudonymisation or Pseudonymised: 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.

Related Policies: the Company's policies, operating procedures or processes related to this Privacy Policy and designed to protect Personal Data.

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.

2.0 Policy Statement

In the provision of products or services to a customer or employment of Company Personnel, Brink's may be required to obtain and/or use or process certain customer information or may be exposed to or come into possession of Personal Data. As the Data Controller of all Personal Data relating to Company 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 Breach, and establish data protection practices as may be practical and/or required under the circumstances.

All lines of business, Brink's entities, and Company personnel are responsible for ensuring all Personal Data is obtained and/or processed in compliance with this Privacy Policy and will implement appropriate practices, processes, controls, and attend training to ensure compliance.

3.0 Data Privacy

3.1 Data Protection Officer

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

The DPO is responsible for overseeing this Privacy Policy and, as applicable, developing Related Policies and Privacy Guidelines. Contact information for The Brink's Company DPO are attached in Appendix B.

For the avoidance of doubt, the overall responsibility of complying with this Privacy Policy lies with the Company and not with the DPO (see Accountability section below).

Please contact The Brink's Company DPO with any questions about this Privacy Policy or the GDPR or with any concerns that this Privacy Policy is not being or has not been followed. In particular, always contact the DPO in the following circumstances:

a) If you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company) (see section 3.3 below);
b) If you need to rely on Consent and/or need to capture Explicit Consent (see section 3.4 below);
c) If you need to draft Privacy Notices or Fair Processing Notices (see section 3.3 below);
d) If you are unsure about the retention period for the Personal Data being Processed (see section 3.8);
e) If you are unsure about what security or other measures you need to implement to protect Personal Data (see section 4 below);
f) If there has been a Personal Data Breach (see section 4.2 below);
g) If you are unsure on what basis to transfer Personal Data outside the EEA (see section 3.9 below);
h) If you need any assistance dealing with any rights invoked by a Data Subject (see section 3.10 below);
i) Whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see section 5.3 below) or plan to use Personal Data for purposes other than what it was collected for;
j) If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see section 5.4 below);
k) If you need help complying with applicable laws when carrying out direct marketing activities (see section 5.5 below); or
l) If you need help with contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see section 5.6 below)

3.2 Personal Data Protection Principles

Brink's adheres to the highest standards relating to Processing of Personal Data which require Personal Data to be:

a) Processed lawfully, fairly, and in a transparent manner (Lawfulness, Fairness, and Transparency).
b) Collected only for specified, explicit, and legitimate purposes (Purpose Limitation)
c) Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed (Data Minimization)
d) Accurate and where necessary kept up to date (Accuracy)
e) 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)
f) 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)
g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation)
h) 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).

3.3 Lawfulness, Fairness, and Transparency

Brink's commits Personal data will only be collected, Processed, and shared fairly, lawfully, transparently, and for specified purposes, including but not limited to:

a) the Data Subject has given his or her Consent;
b) the Processing is necessary for the performance of a contract with the Data Subject;
c) to meet legal compliance obligations;
d) to protect Data Subject's vital interests; or
e) to pursue legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests needs to be set out in applicable Privacy Notices or Fair Processing Notices;

Brink's will provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing 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 collect Personal Data directly from Data Subjects, including for human resources or employment purposes, the Data Subject must be provided with the identity of the Data Controller and DPO, how and why Brink's will use, Process, disclose, protect and retain that Personal Data through a Fair Processing Notice which 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 publically available source), Brink's must provide the Data Subject with all the required information as soon as possible after collecting/receiving the data. 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.

The Brink's organization is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) which has jurisdiction to investigate any claims against The Brink's Company regarding possible unfair or deceptive practices and violations of laws or regulations covering privacy as stated by the Federal Trade Commission.

3.4 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 easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honored. Consent may need to be refreshed 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 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 Data unless required. Where Explicit Consent is required, Brink's will issue a Fair Processing Notice to the Data Subject to capture Explicit Consent. Brink's must evidence Consent captured and keep records of all Consents so that the Company can demonstrate compliance with Consent requirements.

3.5 Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. Personal Data cannot be used for new, different or incompatible purposes from that disclosed when it was first obtained unless Data Subject is informed of the new purposes and they have consented where necessary.

3.6 Data Minimization

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. Company Personnel may only Process Personal Data when performing job duties requires it. Brink's may only collect Personal Data required for job duties; do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes. Ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymized in accordance with the Company's data retention guidelines.

3.7 Accuracy

Brink's must ensure that Personal Data used and held is accurate, complete, kept up to date and relevant to the purpose for which it was collected. Brink's must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data without delay.

3.8 Storage Limitation

Brink's must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which originally collected including for the purpose of satisfying any legal, accounting or reporting requirements.

The Company will maintain retention policies and procedures to ensure Personal Data is deleted in accordance to 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 the Company'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 Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice or Fair Processing Notice.

3.9 Transfer Limitation

Brink's commits to only transfer Personal Data outside the EEA if one of the following conditions applies:

a) 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
b) appropriate safeguards are in place such as 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;
c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
d) the 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.

3.10 Data Subject's Rights and Requests

Data Subjects have rights regarding how Brink's handles their Personal Data. These include rights to:

a) withdraw Consent to Processing at any time;
b) receive certain information about the Data Controller's Processing activities;
c) request access to their Personal Data;
d) prevent use of their Personal Data for direct marketing purposes;
e) 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;
f) restrict processing in specific circumstances;

g) challenge processing which has been justified on the basis of legitimate interests or in the public interest;
h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;
i) object to decisions based solely on Automated Processing, including profiling (ADM);
j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
l) make a complaint to the Privacy Shield Annex I Arbitration Mechanism: Brink's has designated ICDR as U.S.-based third party dispute resolution provider; ICDR can be contacted through their website; http://go.adr.org/privacyshield.html; and
m) 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; do not allow third parties to persuade you into disclosing Personal Data without proper authorization. Forward any employee Data Subject requests received to HR Representative / Department Head immediately upon receipt. Forward any customer Data Subject requests received to Business Representative / Customer Support immediately upon receipt.

The HR Representative will immediately inform the DPO of any data subject access requests and of the action undertaken to handle it.

4.0 Data Security, Integrity, and Confidentiality

4.1 Protecting Personal Data

Brink's commits to maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). Brink's Information Security and Compliance will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. Company Personnel are responsible for protecting the Personal Data held by Brink's and must implement reasonable and appropriate security measures against unlawful or unauthorized Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. Company 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. Company Personnel must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

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

4.2 Reporting a Personal Data Breach

Brink's has put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

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 potential Personal Data Breach should be preserved.

5.0 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:

a) appointing a suitably qualified local DPO where applicable and Global DPO responsible for monitoring GDPR compliance;
b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
c) integrating data protection into internal documents including this Privacy Policy, Related Policies, Privacy Guidelines, Privacy Notices or Fair Processing Notices;
d) regularly training Company Personnel on GDPR, this Privacy Policy, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and
e) 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.

5.1 Record Keeping

Brink's will maintain accurate corporate records reflecting Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with the Company'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's retention period, documented data flows, and a description of the security measures in place.

5.2 Training and Audit

Brink's will provide training for all Company Personnel to enable them to comply with this Privacy 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.

5.3 Privacy by Design and Data Protection Impact Assessment (DPIA)

Brink's must comply with Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organizational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

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

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

Data controllers must also conduct DPIAs in respect to high risk Processing and when implementing major system or business change programs involving the Processing of Personal Data including:

a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
b) Automated Processing including profiling and ADM;
c) large scale Processing of Sensitive Data; and
d) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

a) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;
b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;
c) an assessment of the risk to individuals; and
d) the risk mitigation measures in place and demonstration of compliance.

DPIA findings must be discussed with The Brink's Company DPO.

5.4 Automated Processing (including profiling) and Automated Decision-Making

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

a) a Data Subject has Explicitly Consented;
b) the Processing is authorized by law; or
c) the Processing is necessary for the performance of or entering into a contract.

If certain types of Sensitive Data are being processed, then grounds (b) or (c) will not be allowed but such Sensitive 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 Automated Processing (including profiling) or ADM activities are undertaken.

5.5 Direct Marketing

Brink’s must obtain Data Subject Consent prior to sending electronic direct marketing. The limited exception for existing customers known as "soft opt in" allows Brink’s to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they 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.

5.6 Sharing Personal Data

Company Personnel may only share Personal Data held by Brink’s with another employee, agent or representative of Brink’s affiliates 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:

a) they have a need to know the information for the purposes of providing the contracted services;
b) 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;
c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
d) the transfer complies with any applicable cross border transfer restrictions; and
e) a fully executed written contract - or amendment to an already existing contract - that contains GDPR approved third party clauses has been obtained.

6.0 ANNUAL REVIEW

Brink's reserves the right to change this Privacy Policy at any time without notice. Brink's Global DPO will consistently monitor and periodically audit this Privacy Policy to ensure it complies with the General Data Protection Regulation. Notwithstanding the foregoing, this Privacy Policy will be formally reviewed and updated at least once annually by Brink's Global DPO. In the event the Privacy Policy requires changes due to regulatory or other requirements, then the Privacy Policy will be promptly amended to reflect such changes.

APPENDIX A

All Brink's U.S. entities and subsidiaries that adhere to the Privacy Shield Principles

BAX Holding Company

Brink's Administrative Services Inc.

Brink's Brokerage Company, Incorporated

Brink's C.I.S., Inc.

Brink's Cambodia, Inc.

Brink's Delaware, LLC

Brink's Express Company

Brink's Global Payments, LLC

Brink's Global Services International, Inc.

Brink's Global Services KL, Inc.

Brink's Global Services USA, Inc.

Brink's Holding Company

Brink's International Management Group, Inc.

Brink's Network, Incorporated

Brink's Security International, Inc.

Brink's Ukraine, Inc.

Brink's Vietnam, Incorporated

Brink's, Incorporated

Domesa Courier Corporation

Dunbar Armored, Inc.

Liberty National Development Company, LLC

New Liberty Residential Urban Renewal Company, LLC

Pittston Coal Management Company

Pittston Services Group Inc.

The Brink's Company

The Brink's Company Political Action Committee

The Brink's Foundation

The Pittston Company

APPENDIX B

Data Protection Officer

Brink's Global DPO 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.

DPO Structure: