BRUSCH SERVICES SRL
DATA PROTECTION POLICY

PART ONE: GENERAL BRUSCH SERVICES SRL
DATA PROTECTION POLICY
REQUIREMENTS FOR ALL STAFF

PURPOSE

1.1 This document sets out the policies and procedures that the BRUSCH SERVICES SRL has put in place to comply with basic data protection principles. Because BRUSCH SERVICES SRL are situated in Europe, this document especially takes into account European data protection laws and provides a short overview of these laws – especially the European Data Protection Directive (Directive 95/46/EC) respectively the EU General Data Protection Regulation (EU) 2016/679 ("**GDPR**") from 25 May 2018 onward.

2. **SCOPE**

2.1 This policy applies to Brusch Services SRL and all of its branches and entities worldwide (together "**BRUSCH SERVICES SRL**"). All employees and agency personnel (staff) within BRUSCH SERVICES SRL must comply with the policy. All BRUSCH SERVICES SRL staff will receive information security training (which includes data protection compliance) on a regular basis.

2.2 Some parts of this policy apply to the branches and entities situated in EU only.
2.3 This policy is split into two parts: Part One is general and applies to all staff. Part Two contains additional provisions for specific departments and operations in specific countries. More detailed provisions apply to:

 Annex A: Personnel Department;

 Annex B: Sales and Procurement;

 Annex C: Information Technology;

 Annex D: Facilities.

2.4 Data protection laws vary from country to country. This policy has been reviewed for local compliance in Australia, British Virgin Islands, Bulgaria, Canada, China, Cyprus, Denmark, France, Germany, India, Luxembourg, Malaysia, Mexico, The Netherlands, Poland, Romania, Russia, Singapore, South Africa, Sweden, Switzerland, UK, Ukraine, USA and Vietnam. Where there is a different requirement in these countries, a note is indicated above the text and you must refer to the relevant country-specific Appendix in Part Two.

3. **COMMITMENT TO COMPLY WITH BASIC DATA PROTECTION PRINCIPLES**

3.1 All BRUSCH SERVICES SRL staff must comply with their obligations under this policy and applicable local data protection laws whenever they are processing personal data. The Data Protection Safeguards set out in Section 4 below and in Part Two set out what this means.
3.2 **Data protection principles apply when personal data is processed by, or on behalf of, BRUSCH SERVICES SRL.**
3.3 'Personal data' has a broad meaning: all information that relates to living, identifiable, individuals (either directly or indirectly). This includes data that would identify a person (name, address, telephone or employee number, etc). It includes opinions about individuals as well as facts. Personal data can include information about employees and business contacts: it is not confined to consumers or to a person's personal (i.e. non-work) life either: job title, office telephone number and professional details (for example) are also personal data. The fact that information is publicly available (e.g. on LinkedIn) does not stop data protection laws applying to it.
3.4 'Processing' also has a broad meaning: for example, it covers collection of data, holding and using data and destroying personal data. All BRUSCH SERVICES SRL staff will almost certainly process some personal data: about customers or suppliers, or about other employees.

3.5 Basic data protection principles require that BRUSCH SERVICES SRL:

 only processes personal data for fair and lawful purposes;
 in accordance with additional restrictions for sensitive personal data1;
 is transparent with people and tells them how it will use their information;
 meets data quality obligations and holds personal data for a limited retention period;

 as a general rule minimizes the amount of personal data it collects and processes and chooses and structures its processing systems accordingly;
 as a general rule grants its staff access to personal data on a “need to know” basis only;
 Implements appropriate security obligations to protect personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures;
 upholds individuals’ rights to access and correct their information and, to prevent certain types of processing;**]** and
 only transfer personal data to other jurisdictions than their own when protections for personal data are in place as required by local law (e.g. European Operations only transfer personal data out of the European Economic Area (EEA)2 and Switzerland when protections for personal data are in place such as the standard contractual clauses provided by the EU Commission).

3.6 Data protection laws often also require that BRUSCH SERVICES SRL must notify its processing of personal data to the local data protection authority. The appropriate Data Protection Officer is responsible for ensuring that this is done.
3.7 Section 4 sets out the steps BRUSCH SERVICES SRL has adopted and that you must follow to ensure that these obligations are met.

4. LAWFUL PORPOSE

4.1.1 BRUSCH SERVICES SRL may only process personal data for explicit and legitimate purposes and does not further process data in a manner that is incompatible with those purposes.
4.1.2 Generally, staff may process personal data (other than sensitive personal data) where (1) this is necessary for BRUSCH SERVICES SRL SRL's legitimate interests (as defined by local law), provided this does not cause unreasonable prejudice to the interests of the individuals concerned (2) processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract or (3) processing is necessary to comply with a legal obligation.
4.1.3 In some situations, BRUSCH SERVICES SRL may also process personal data when the relevant individual has given consent. This must usually be express and in many countries this is subject to strict formal requirements. Marketing may process personal data on this basis. In other situations, staff should seek guidance from the Data Protection Officer if they wish to collect and use personal data based on individual consent.

Where BRUSCH SERVICES SRL holds personal data for certain specific purposes, staff must not then use the data any other way which is incompatible with those purposes: if the relevant individuals would not expect this use of the data, it is likely to be 'incompatible use'. For example, you may not access the customer or staff databases for your own purposes, or for friends or family. This is a serious disciplinary offence and may be a criminal offence for which you can be prosecuted.
4.1.5 Use of data for a new purpose, can also affect BRUSCH SERVICES SRL SRL's filings with data protection authorities. Staff must therefore consult the Data Protection Officer, if they wish to use personal data for a new purpose.

Sensitive personal data

Sensitive personal data is generally information about an individual's physical or mental health or condition, racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs and sexual life, genetic and biometric data (if this data is processed for the purpose of uniquely identifying an individual) although local laws may vary (for example in the UK, the commission or alleged commission of any criminal offence and criminal convictions are also sensitive personal data and in Poland sensitive personal data includes data relating to decisions issued in court or administrative hearings).

Transparency

BRUSCH SERVICES SRL must be transparent about how it uses personal data: if you collect personal data about individuals, you must tell them how this information will be used. This means providing information about:

 the BRUSCH SERVICES SRL entity collecting the information (including the contact data of the Data Protection Officer, where applicable);

 the purposes for which BRUSCH SERVICES SRL SRL processes personal data as well as the legal basis for the processing;

 where the data processing is based on legitimate interests, the legitimate interests of BRUSCH SERVICES SRL SRL on which the data processing is based;

 whether replies to questions are mandatory or voluntary, and the consequences if information is not provided;

 the types of people who will receive the data and the purposes for which they will receive it;

 the rights that individuals have (including to access, correct and sometimes to object to the processing of their data); and

 any transfers of personal data outside their own jurisdiction, where required by local law; European Operations have to provide information about any transfers of personal data outside EEA.

4.3.2 In addition to the information referred to in Section 4.3.1, the BRUSCH SERVICES SRL shall, at the time when personal data are obtained, provide individuals with the following further information necessary to ensure fair and transparent processing in accordance with applicable data protection laws:
 the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

 the existence of the right to request from BRUSCH SERVICES SRL access to and rectification or erasure of personal data or restriction of processing concerning individuals or to object to processing as well as the right to data portability;

 if the data processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

 the right to lodge a complaint with a supervisory authority;

 whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether an individual is obliged to provide the personal data and of the possible consequences of failure to provide such data;

 the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for an individual;
4.3.3 Where personal data have not been directly obtained from an individual, and in accordance with applicable data protection laws, the BRUSCH SERVICES SRL shall provide the individual with the following information in addition to the information as set out in 4.3.2:
 the categories of personal data concerned;

 from which source the personal data originate, and if applicable, whether it comes from publicly accessible sources.

4.3.4 In general, the information set out under the foregoing sections must be provided to individuals before BRUSCH SERVICES SRL obtains personal data from them. BRUSCH SERVICES SRL does not have to provide this information to the extent the individual already has the information. Specific requirements for Personnel Department and Marketing are set out in the relevant Annexes
4.3.5 It is not necessary to provide this information for business contact information provided by the individual, where it is evident from the context how you will use the information (e.g. giving a card to allow for follow up).

Data quality and retention

You should only use personal data that are adequate, relevant and not excessive. Data may only be collected if there is a business need for the information and if the level of information is proportionate to this.

4.4.2 You should use personal data that are accurate and, where necessary, up to date. You should advise Personnel Department promptly if your details change. If you are told about a change in a customer's or supplier's personnel, you should change any local contact databases that you maintain and ensure central databases are updated accordingly.
4.4.3 BRUSCH SERVICES SRL must not retain personal data for longer than is necessary for the purposes for which the data was collected. Guidance on what this means for Personnel Department is set out in Annex

Security and confidentiality

BRUSCH SERVICES SRL shall implement appropriate administrative, technical, organizational and physical measures to protect personal data, including *inter alia*,
 the pseudo nomination and encryption of personal data;

the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

 the ability to restore the availability and access to personal data in a timely manner in the event of a data breach;

 a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
4.5.2 This requires appropriate IT and physical security and staff training and care in selection of third parties who process BRUSCH SERVICES SRL personal data. These measures may vary from country to country.
4.5.3 BRUSCH SERVICES SRL shall, where required and in accordance with applicable laws, carry out data protection impact assessments (“PIA”) before introducing new processing operations.
4.5.4 The main processes for securing the BRUSCH SERVICES SRL SRL IT environment are set out in the Information Security Manual, Security Incident Management policy and associated documents, which all staff must comply with. Further guidelines are set out in the Corporate Code of Conduct, the Insider Trading Policy, the Rules for Handling of Service Information, the Regulations on the Processing of Personal Data, Rules on Company Information Treatment by Employees, Instructions “Use of Corporate Electronic Mail” and Non-disclosure agreements.

4.5.5 Where staff have permission to work from home or any other off-premises site, special conditions apply to the handling of personal data which must be fully observed.
4.5.6 Any suspected or actual breach, unauthorized disclosure of, damage to or loss of any BRUSCH SERVICES SRL personal data (including loss of or damage to equipment containing BRUSCH SERVICES SRL personal data) shall be reported immediately to the Chief Information Officer (CIO) or to the IT Department as well as to the appropriate Data Protection Officer.

Restrition on transfers outside the EEA

European data protection rules restrict transfers of personal data to including SRL companies in countries that are outside the European Economic Area (EEA)**3** and Switzerland unless prescribed steps are taken to ensure that the data is protected. Since some of BRUSCH SERVICES SRL SRL's IT applications are held and backed outside the EEA and Switzerland, this restriction is particularly relevant for its European Operations.
4.6.2 BRUSCH SERVICES SRL has put in place European Commission approved agreements to regulate the transfers of certain categories of data within the BRUSCH SERVICES SRL of companies.
4.6.3 European Operations staff must seek the input of the Data Protection Officer if you want to transfer personal data to a new supplier outside the EEA or Switzerland or if you want to transfer new categories of data to BRUSCH SERVICES SRL entities outside the EEA or Switzerland. The input of the Data Protection Officer must include the information whether prior notification or authorization of the transfer by the competent data protection authority is required.
Each individual shall have the right to obtain from BRUSCH SERVICES SRL confirmation as to whether or not personal data concerning the individuals are processed, and, where that is the case, access to the personal data and the following information:
 the purposes of the processing;
 the categories of personal data concerned;
 the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;
 where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

 the existence of the right to request from BRUSCH SERVICES SRL rectification or erasure of personal data, restriction of processing personal data concerning the individual, and to object to such processing;
 the right to lodge a complaint with a supervisory authority;
 where personal data are not collected directly from the individual, any available information as to their source;
 the existence of automated decision-making, including profiling.

4.7.2 Where personal data are transferred to a third country or to an international organization, the individual shall have the right to be informed of the appropriate safeguards relating to the transfer.
4.7.3 BRUSCH SERVICES SRL will always honor individuals' rights under and according to data protection laws:
 correct information relating to them;
 to erasure ("right to be forgotten");
 to data portability;
 to restriction of processing;
 to prevent direct marketing to them;
 to prevent certain other types of processing in special situations; and
 to object to the use of entirely automated decisions to take significant decisions about them.
4.7.4 Staff must take care when entering information in free-text areas as those to whom the text refers (such as customers) may see this information at a later date. Information should only be entered which is appropriate and justifiable and should not include sensitive personal data.
4.7.5 Requests by staff to see their records should be made, in writing, to the Head of Personnel Department. If staff receives any other request to see personal details or a request that BRUSCH SERVICES SRL delete data or cease processing data should be forwarded immediately to the Data Protection Officer. There are often strict timescales for complying with such requests, so requests must be forwarded as soon as possible following receipt.
5. **EXCEPTIONS:**
Any request to deviate from this policy must be approved by the Data Protection Officer.
VIOLATIONS:

6.1 Subject to local law requirements, failure to comply with this policy may be a disciplinary offence and will be handled in accordance with BRUSCH SERVICES SRL's disciplinary procedures.
6.2 Failure to comply with this policy may also mean that you are directly liable for penalties under local data protection law. In particular, use, for private or illegal purposes, of personal data obtained through your work at BRUSCH SERVICES SRL can be a criminal offence.
7. **ANY QUERIES?**
If you have any queries in relation to this policy or data protection generally, you should contact your appropriate Data Protection Officer.
8. **APPROVAL AND VARIATION**
This policy has been approved by Board of Directors of Brusch Services SRL. The Data Protection Officer is the sponsor for this policy and must approve any changes to it.

PART TWO: DEPARTMENT OR COUNTRY SPECIFIC GUIDANCE
CONTENTS

ANNEXES

Annex A: Personnel Department

Supplementary Document 1: Sample Data Protection Notice for Applicants
Supplementary Document 2: Sample Privacy Notice for Employees
Supplementary Document 3: Personnel Department Records Retention Periods
Supplementary Document 4: Sample Data Processor Wording
Annex B: Sales and Procurement
Annex C: Information Technology
Annex D: Facilities
COUNTRY: Romania

Annex A – Personnel Department

DATA PROTECTION SAFEGUARDS
LAWFUL PURPOSES

Normal data	Some of BRUSCH SERVICES SRL's contracts of employment currently ask for employee consent to data processing. However, in most countries BRUSCH SERVICES SRL is entitled to process information about applicants and employees where: it is necessary for its legitimate interests; this is required to meet statutory obligations or to administer the employment contract.
Sensitive data	BRUSCH SERVICES SRL is entitled to process sensitive personal data about employees where this is necessary to comply with obligations under employment law – such as dealing with statutory sick pay, or making work-place adjustments

Keep sickness and accident records separate from absence records, so absence records do not contain sensitive personal data.

Criminal offences	Do not ask applicants for details of criminal offences unless this is necessary for the position. Generally, only unspent convictions will need to be requested. Seek local advice before asking for criminal offence data outside the UK.
New Uses	Use of data for a new purpose, can also affect BRUSCH SERVICES SRL's filings with data protection authorities (e.g new Personnel Department database or system). It may also require consultation with workers' representatives. Staff must therefore consult the Data Protection Officer, if they wish to use personal data for a new purpose.

TRANSPARENCY

Applicants

Ensure that all applicants are told how BRUSCH SERVICES SRL will use CVs and other personal data.

For unsuccessful applicants, explain if you want to keep CVs on file for future use and do not do this if the applicant objects.

For successful applicants, be clear what background checks will be made and from whom the information will be sought (e.g. identification checks, certification of right to work, collection of references). Make it clear if the successful completion of background checks is a pre-condition of employment with BRUSCH SERVICES SRL.

Refer to the standard notice for applicants at Supplementary Document 1.

Employees

Ensure all staff are told how BRUSCH SERVICES SRL uses their personal data: relevant information should be included in the Employee Privacy Notice (see Supplementary Document 2).

Where BRUSCH SERVICES SRL provides staff data to third parties to provide benefits, make staff aware of this in the literature used to explain the benefits (e.g. pension, insurance or private health providers). If BRUSCH SERVICES SRL collects information to pass on to the third parties for administration purposes, do not use this for general employment purposes.

DATA QUALITY

General

Only collect information about individuals where there is a clear and foreseeable need for the information.

Ensure that when you collect information in application forms/new joiner forms that you identify what information is mandatory or what information is voluntary (i.e by way of a footnote).

Applicants

If you prepare an application form, only request information which is relevant and not excessive. It should also comply with all relevant anti-discrimination laws.
Remind interviewers that they should only record information during an interview which is relevant to the recruitment decision: applicants may have a right to see interview notes.

RETENTION

General
Carry out file reviews and ensure that irrelevant information is removed and securely destroyed.
Follow the retention guidelines at Supplementary Document 3.

SECURITY

You should ensure that:
 only staff needing access to personnel files to carry out their duties are given such access, and audit trails are put in place to show who has accessed and/or amended such files;
 the taking of employee personal data off-site (e.g. in laptop computers) is controlled and that strict security rules are applied;
 if you are sending confidential or sensitive information about an employee by email or fax, consider whether additional security measures such as encryption are required.

TRANSFERS
Seek advice from the Data Protection Officer if:
you wish to use a third party outside your own jurisdiction to process employee personal data; or
if you belong to European Operations and
 wish to use a third party outside the EEA or Switzerland or
 have any queries about what data may be transferred to BRUSCH SERVICES SRL entities outside the EEA or Switzerland.

RIGHTS
Access
Forward any requests from candidates or employees to see and/or correct their data or to object to the processing of their data to the Head of Personnel Department. Remind line managers to do this.
Seek the advice of the Data Protection Officer, if needed, in handling subject access requests.

SPECIAL SITUATIONS

Requests to disclose data
References: always check with the employee before providing a reference.
If asked to disclose information about an employee to a third party, always verify the identity of the third party to check they are entitled to receive the information. Consider whether there is a legal obligation to disclose the information (e.g. in the UK to the Inland Revenue) or whether information is required for legal proceedings or in connection with the prevention or detection of crime. If these considerations do not apply, consider whether it would be fair to the employee to release the information. Please seek further advice from the Data Protection Officer if you are uncertain about the nature of the request.
Where practicable, workers should be told about such disclosures.

Monitoring
The Head of Personnel Department must authorize any requests to monitor specific employees. This would apply to any of monitoring IT Equipment and traffic on the IT Network telephone calls and other forms of monitoring. Before authorizing any monitoring, the Head of Personnel Department will:

 Carry out an impact assessment, to ensure that there is a legitimate purpose for the monitoring, that the impact of the monitoring on the individual is justified and that the intrusiveness of the monitoring is kept to the minimum level necessary to achieve the purpose of the monitoring;
 Consider if employees should be notified that monitoring will be carried out. Where monitoring is used to enforce BRUSCH SERVICES SRL rules and policies, the relevant rules and policies and the nature and extent of associated monitoring must be clearly specified. General notice to this effect is included in the Rules on Company information treatment by employees, Information Security Manual and the Employee Privacy Notice;
 Consider any applicable local law requirements relating to monitoring and interception, particularly as this can constitute a criminal offence in certain countries. In some countries, the works council may also need to be consulted;
 Ensure that the results of employee monitoring will only be available to a limited number of people and may only be used for the purpose for which the monitoring was implemented, unless the results reveal evidence of criminal activity at work, gross misconduct or breaches of health and safety rules which no reasonable employer could ignore; and
 Ensure that emails which are clearly marked as personal will only be read in exceptional circumstances where a problem relating to an employee's excessive or unauthorized use is suspected. You should always contact the appropriate Data Protection Officer and Legal Department before doing so. Note that in some countries, it is prohibited to read any emails marked as private. Please consult the relevant Country Appendices. **Also refer to the local rules for further information.**

SUPPLEMENTARY DOCUMENT 1: SAMPLE DATA PROTECTION NOTICE FOR APPLICANTS

BRUSCH SERVICES SRL is committed to respecting your privacy. We will treat any personal information supplied by you in this application form as confidential and will only process such information as permitted by the Data Protection Act 1998 and as described below.
What information do you have to provide?
If you wish us to consider your application, you have to submit your CV and any other information.
Additional wording where details of criminal convictions are requested:
Where permitted by law, if we ask you to supply information about your criminal record you do not need to supply details of spent convictions5.

Additional wording required where sensitive personal data is collected:
The Data Protection Act 1998 gives special protection to information about racial/ethnic origin, political opinions, religious beliefs, trade union memberships, health, sexual life and the commission of offences and related proceedings. You should only provide this information if it is required in response to a mandatory question on our website, or if you are otherwise content for us to process this information. We will always hold such information securely.

How do we use this information?
We will use the information you have provided in order to assess your suitability for BRUSCH SERVICES SRL.
Additional wording required where the applicant may be considered for a number of jobs in addition to the advertised job:
If we think that you are suitable for other current vacancies, we may also use the information you have provided for this purpose. We will retain your information for 6 months.
Additional wording where the application form will be kept for possible future use:
If we fill the vacancy for which you have applied, we may keep your application on file for 12 months in case we think you are suitable for other, similar, vacancies in the future. Please let us know if you do not wish us to retain your data for this purpose.
Additional wording where information in the application form will be verified:
We will make the following checks of the information you have provided in the form:
 Checks of experience by contacting previous employers;
 Checks of academic credentials by contacting educational institutions; and
 Checks of the Disclosure and Barring Service.

If we wish to make any other checks (such as to take up references) we will seek your permission first.
Additional wording where vetting will be carried out:
In addition to the checks described above, we will make enquiries of third parties about your background and circumstances. These checks are necessary, as this post involves access to confidential information and/or requires security clearances. In order to carry out these checks we will: [explain nature of checks to be carried out, the nature, extent and range of sources that will be checked, what information will be released to third parties and when the checks will be carried out].

We are an international company and we provide software services. Accordingly, where we think it appropriate, we may transfer the information we receive from you to our clients deserved by BRUSCH SERVICES SRL. Some of these clients may not have equivalent data protection legislation to Europe. However, whenever we transfer your data in this way, we will transfer it in accordance with the applicable EU data protection requirements, keep it secure and only use it as outlined in this notice.

Drafted to comply with the UK law only. Amendments will be required to use in other countries:
BRUSCH SERVICES SRL, 15 New Tipografilor Street, Sibiu, Romania ("BRUSCH SERVICES SRL"), is committed to respecting your privacy. We will only process such information as permitted by the Data Protection Act 1998 and as described below.

What information do we collect about you?
The information we collect about you includes:
 your name, home address, postal address, temporary address, nationality, employee ID number, national insurance number, immigration status, age, data of birth, passport and ID number, photo image,
 beneficiaries' details in relation to life insurance or other benefits, emergency contacts, marital status, information about family members (name, date of birth, gender and national personal ID number) where necessary for the provision of applicable benefits, alimony payments, guarantees or relocation assistance,
 job title, employer, division, position, business unit, location of working place, work email, professional experience, education, performance history, training records,
 health insurance details, salary, remuneration, social and other benefits, bank details
 trip itineraries with dates and times, visa, driving license details,
 expense records (such as details of out of pocket expenses, corporate credit cards, company cars or private cars where an allowance is claimed and mobile phone costs),
 phone numbers (home and mobile), written and electronic communications, where permissible
 information concerning performance, career plans, conduct and, where permissible, about violation of laws or breach of company policies,
 medical leave information, sickness and accident records, medical certificates, workplace adjustments, other documents required to confer special benefit status, such as information concerning pregnancy status and age of children, etc. where applicable and
 information about trade union affiliation if you have asked us to make payments to trade unions on your behalf.

BRUSCH SERVICES SRL will keep this information, together with data retained from the application and selection process, for the course of the employment relationship and, to the extent permitted, after termination of employment.

How do we use this information?

BRUSCH SERVICES SRL processes this personal data for the following purposes:
 As required to establish and perform the employment contract, to maintain or terminate the employment relationship and to enable you to perform your job. This includes recruiting and hiring and administration of payroll and benefits, absence, compensation and sales quota commission, performance and talent management, training and leadership development, transfer management from different subsidiaries and branches, succession management, award recognition, employee surveys, medical insurance, occupational health, retirement plans, stock plans, expense management, activity at client's locations and professional travel.

 As required by BRUSCH SERVICES SRL to enable its business, in particular to provide access to BRUSCH SERVICES SRL' s offices, management of BRUSCH SERVICES SRL's IT systems and infrastructure, inclusion in company directories and provision of communication services such as e-mail, telephone and internet access.

 Protecting the security of BRUSCH SERVICES SRL's premises, assets, systems, and intellectual property and enforcing company policies, including monitoring communications where permitted by local law and in accordance with BRUSCH SERVICES SRL's Regulations on the processing of personal data, Rules on Company information treatment by employees, Information Security Manual, Security Incident Management, Instructions "Use of Corporate Electronic Mail" and for investigations and disciplinary actions.

 Compliance with applicable laws and protection of BRUSCH SERVICES SRL's legitimate business interests and legal rights, including, but not limited to, use in connection with legal claims, compliance, regulatory, investigative and disciplinary purposes (including disclosure of such information in connection with legal process or litigation) and other ethics and compliance reporting tools.

In addition, with your consent, we collect your picture for use with your contact details in BRUSCH SERVICES SRL directories, in internal communications and newsletters and in external news and media in connection with events and updates about BRUSCH SERVICES SRL. Where permitted by local law and with your consent, we also hold background checks to evaluate eligibility for employment and medical information if a regular or onboarding health check is required or to evaluate eligibility for applicable benefits.
Personal data will be transferred to Brusch Services SRL, its affiliates and contractors, in the US and other countries, including outside the EU, and will be stored and processed manually and electronically through global systems and tools for the purposes above. Information contained in internal directories may be accessed on a worldwide basis by employees of other BRUSCH SERVICES SRL entities. Other personal data will primarily be processed by employees of the HR, IT and finance, legal and facilities departments, where relevant and necessary. We have taken steps to ensure that there is adequate protection for your personal data in these circumstances. Personal data may be shared with government authorities and/or law enforcement officials if required for the purposes above, if mandated by law and if required for the legal protection of BRUSCH SERVICES SRL's legitimate interests in compliance with applicable laws. Personal data may also be shared with third party service providers, who will process it on behalf of BRUSCH SERVICES SRL for the purposes above. Such third parties include, but are not limited to, payroll service providers, IT service providers, travel agencies and travel service providers, banks, credit card companies, brokers, medical services and medical insurance providers, training providers, survey service providers, investigators, employee hotline administrators, data custodians, etc. In the event that the business is sold or integrated with another business, your details may be disclosed to our advisers and any prospective purchaser's adviser and will be passed to the new owners of the business.
BRUSCH SERVICES SRL has taken appropriate technical, administrative, physical and procedural security measures, consistent with local and international information practices, to protect the personal data from misuse, unauthorized access or disclosure, loss, alteration, or destruction. These measures include:
 Physical safeguards, such as locked doors and file cabinets, controlled access to our facilities, and secure destruction of media containing personal data.
 Technology safeguards, such as use of anti-virus and endpoint protection software, passwords, encryption, and monitoring of our systems and data centers to ensure compliance with our security policies.
 Organizational safeguards, through training and awareness programs on security and privacy, to ensure employees understand the importance and means by which they must protect personal data, as well as through privacy policies and policy standards that govern how BRUSCH SERVICES SRL treats personal data.

Your rights

According to the Data Protection Act 1998, you have the right to access or rectify personal data that relates to you. To rectify or request access to your personal data please contact your HR representative at any time. There are exceptions to these rights so that access may be denied, for example, if making the information available would reveal personal information about another person or if BRUSCH SERVICES SRL is legally prevented from disclosing such information. You have the right to withdraw your consent at any time with future effect. In that case, however, we may still process your personal data on an alternative legal basis in accordance with applicable data protection laws.

Your obligations

It is important that we maintain up to date records of key information on you. Please notify your manager of any changes in your personal circumstances as soon as they occur (eg change of address, marital status, emergency contacts). From time to time we may ask you to complete a new personal information form to ensure our records are up to date.

Where we require personal data to comply with legal or contractual obligations, then provision of such data is mandatory: if such data is not provided, then we will not be able to manage the employment relationship, or to meet obligations placed on us. In all other cases, provision of requested personal data is optional.

Consent to use of photo
Please confirm by ticking the boxes below if you agree to your photo being used for the following purposes:

[ ] corporate directory;
[ ] internal communications and newsletters;
[ ] external news and media (including online media) in connection with events and updates about BRUSCH SERVICES SRL SRL.

_____ _____
Date Name of employee

SUPPLEMENTARY DOCUMENT 4: SAMPLE DATA PROCESSOR WORDING

Set out below is some precedent data processor wording which should be added to contracts where a BRUSCH SERVICES SRL entity is appointing a service provider who will be processing personal data on behalf of the respective BRUSCH SERVICES SRL entity (e.g archive companies, hosting or support providers). The clauses have been drafted on the assumption that they will be included in a longer contractual document. These have been drafted to comply with the provisions relating to processors set out in the European Data Protection Directive (Directive 95/46/EC), respectively the EU General Data Protection Regulation (EU) 2016/679 ("**GDPR**") upon applicability..
Additional provisions may be required where the BRUSCH SERVICES SRL entity, whose data is being processed, is based in Canada, Germany, Luxembourg, Poland, South Africa, Sweden or Switzerland. In this situation, please speak to the Data Protection Officer before using these clauses.

1 Data Protection
1.1 The parties' attention is drawn to Directive 95/46/EC of the European Parliament and any legislation and/or binding regulations implementing them or made in pursuance of them (all referred to together as the "Data Protection Requirements").
1.2 It has been agreed between the parties that the Service Provider [BRUSCH SERVICES SRL entity processing data on behalf of other BRUSCH SERVICES SRL entity] will under contract to and on behalf of [insert relevant BRUSCH SERVICES SRL entity] ("**BRUSCH SERVICES SRL Entity**") process certain personal data of Controller ("**BRUSCH SERVICES SRL Entity's Personal Data**").
The Service Provider acknowledges that BRUSCH SERVICES SRL Entity is the data controller in respect of BRUSCH SERVICES SRL Entity's Personal Data that the Service Provider processes in the course of providing services for BRUSCH SERVICES SRL Entity, and that the Service Provider is the data processor in respect of BRUSCH SERVICES SRL Entity's Personal Data.
1.3 The Service Provider agrees that it shall:

(a) only (i) carry out processing of BRUSCH SERVICES SRL Entity's Personal Data in accordance with BRUSCH SERVICES SRL Entity's instructions as set out in this Agreement and in particular as set out in Annex 1 or as those instructions may be amended from time to time and (ii) comply with instructions from BRUSCH SERVICES SRL Entity to rectify, erase and/or block BRUSCH SERVICES SRL Entity's Personal Data;
(b) agree with BRUSCH SERVICES SRL Entity and implement appropriate technical and organizational measures to protect BRUSCH SERVICES SRL Entity's Personal Data against unauthorized or unlawful processing and accidental destruction or loss, including without limitation the measures set out in Annex 2 or such other measures as may be agreed between the parties;
(c) use all reasonable endeavors to advise BRUSCH SERVICES SRL Entity if, in the light of new technology and methods of working, BRUSCH SERVICES SRL Entity should consider revising the security methods specified in Annex 2;
(d) not sub-contract any processing of BRUSCH SERVICES SRL Entity's Personal Data without the prior written consent of BRUSCH SERVICES SRL Entity; [***Note: please speak to the Data Protection Officer if sub-processing is required.]***
(e) immediately refer to BRUSCH SERVICES SRL Entity any requests, notices or other communication from data subjects, data protection authorities or any other law enforcement authority, for BRUSCH SERVICES SRL Entity to resolve;
(f) at no additional cost, provide such information to BRUSCH SERVICES SRL Entity as BRUSCH SERVICES SRL Entity may reasonably require, and within the timescales reasonably specified by BRUSCH SERVICES SRL Entity, to allow BRUSCH SERVICES SRL Entity to comply with the rights of data subjects, including subject-access rights, or with notices served by any data protection authority;
(g) not transfer any of BRUSCH SERVICES SRL Entity's Personal Data outside of the European Economic Area without the prior written consent of BRUSCH SERVICES SRL Entity; [***Note: please speak to the Data Protection Officer if a transfer of data is required.]***
(h) represent and warrant that its collection, access, use, storage, disposal and disclosure of BRUSCH SERVICES SRL Entity's Personal Data does and will comply with all applicable federal, state, provincial, local, and foreign privacy and data protection laws, as well as all other applicable regulations and directives; and on the termination of this Agreement and at the choice of BRUSCH SERVICES SRL Entity, return all of BRUSCH SERVICES SRL Entity's Personal Data to BRUSCH SERVICES SRL Entity or destroy all of BRUSCH SERVICES SRL Entity's Personal Data and certify to BRUSCH SERVICES SRL Entity that it has done so, unless prevented from doing so by applicable laws. In that case, the Service Provider warrants that it will guarantee the confidentiality of BRUSCH SERVICES SRL Entity's Personal Data and will not actively process such personal data anymore.

1.4 The Service Provider shall, at no additional cost, keep or cause to be kept full and accurate records relating to all processing of BRUSCH SERVICES SRL Entity's Personal Data on behalf of BRUSCH SERVICES SRL Entity, including but not limited to the records specified in Annex 3, and shall, upon reasonable notice, grant BRUSCH SERVICES SRL Entity and its auditors and agents, a right of access to and to take copies of such records in order to assess whether the Service Provider has complied with the provisions of Clause [1.3]. The Service Provider shall, upon reasonable notice, allow BRUSCH SERVICES SRL Entity and its auditors and agents access to premises and other materials and to its personnel and shall provide all reasonable assistance in order to assist BRUSCH SERVICES SRL Entity and its auditors and agents in exercising its audit rights under this Clause. Service Provider's obligations under this Clause shall continue throughout the Agreement and for a period of six (6) years thereafter.

ANNEX 1: INSTRUCTIONS
This should include any specific instructions with which the Service Provider is required to comply (for example, using specific fair-obtaining notices).

ANNEX 2: SECURITY MEASURES

This should list any agreed security measures here – we have set out some examples below:

1. Access control to premises and facilities
Unauthorized access (in the physical sense) must be prevented.
Technical and organizational measures to control access to premises and facilities, particularly to check authorization:
□□Access control system
□□ID reader, magnetic card, chip card
□□(Issue of) keys
□□Door locking (electric door openers etc.)
□□Surveillance facilities
□□Alarm system, video/CCTV monitor
□□Logging of facility exits/entries.
2. Access control to systems
Unauthorized access to IT systems must be prevented.
Technical (ID/password security) and organizational (user master data) measures for user identification and authentication:
□□Password procedures (incl. special characters, minimum length, change of password)
□□No access for guest users, no anonymous accounts
□□Access to systems centrally managed and restricted to approval by both personnel management and system owner.
3. Access control to data
Access through IT systems outside the allocated access rights must be prevented.
Requirements-driven definition of the authorization scheme and access rights, and monitoring and logging of accesses:
□□Differentiated access rights (profiles, roles, transactions and objects)
□□Access rights defined according to duties and least privilege concepts
□□Log of user access via IT systems.

4. Disclosure control
Aspects of the disclosure of personal data must be controlled: electronic transfer, data transport, transmission control, etc.
checking:
□□All data is transferred via wholly-owned private network
□□Encryption/tunneling (VPN = Virtual Private Network) for remote access, transport and communication of data.
□□Prohibition of use of portable media.

5. Input control
Full documentation of data management and maintenance must be maintained.
Measures for subsequent checking whether data have been entered, changed or removed (deleted), and by whom:
Example:
□□Systems log user activities according to the data importer's security logging standard.

6. Job control
Commissioned data processing must be carried out according to instructions.
Measures (technical/organizational) to segregate the responsibilities between the data exporter and the data importer:
□□Unambiguous wording of the contract
□□Formal commissioning (request form)
□□Criteria for selecting the data importer
□□Monitoring of contract performance.

7. Availability control
The data must be protected against accidental destruction or loss.
Measures to assure data security (physical/automated):
□□Backup procedures
□□Uninterruptible power supply (UPS)
□□Remote storage
□□Anti-virus/firewall systems.

8. Segregation control
Data collected for different purposes must also be processed separately.
Measures to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes:
Examples:
□□Restriction of access to data stored for different purposes according to business function of staff.
□□Segregation of business systems for different purposes
□□Segregation of testing and production environments.
This should also include any policies or procedures adopted by the Service Provider that influenced BRUSCH SERVICES SRL Entity in its selection of the Service Provider and with which BRUSCH SERVICES SRL Entity requires the Service Provider to comply during the contract. For example, if BRUSCH SERVICES SRL Entity was influenced by the fact that the Service Provider meets the British Standards Institute data security standard, ISO/IEC 27001, then this should be referenced here.
The Act requires a data controller to choose a data processor that provides "sufficient guarantees" in relation to security and to take reasonable steps to ensure compliance with these security measures. One way in which BRUSCH SERVICES SRL Entity can take steps to ensure compliance is to list such security measures in the contract, so that, for example, there is an ongoing obligation on the data processor to meet ISO/IEC 27001.

9. Training
Service Provider must adopt the necessary measures to ensure that its staff are aware of security standards and privacy laws. Therefore staff of [*Service Provider*] will receive regular training on the application of privacy laws and security standards.

10. Audits
Service Provider must carry out audits to ensure that the measures set out in this document are complied with.

ANNEX 3: RECORDS
List any records to be kept by the Service Provider and the ways in which they will be made available to BRUSCH SERVICES SRL Entity (e.g. regular despatch, BRUSCH SERVICES SRL Entity's right of entry on the Service Provider's premises, etc.).

Annex B – Sales and Procurement Departments

TRANSPARENCY
You should always ensure that BRUSCH SERVICES SRL is transparent about the use of personal data of business contacts.

SECURITY
BRUSCH SERVICES SRL entities acting as processor

You should always ensure that appropriate confidentiality and data protection clauses are included in contracts that you negotiate with customers. For example, it may be that a BRUSCH SERVICES SRL entity is actually processing personal data on behalf of a customer (e.g. where it is providing support and

maintenance services which require access to a customer's database). In this case, it is for the customer to comply with the relevant data protection laws and to satisfy themselves that BRUSCH SERVICES SRL entity's procedures are adequate. It is important to ensure that standard language is included where required. Please contact the Data Protection Officer if you have any questions regarding the use of such wording.

TRANSFERS

Any new requests to transfer personal data outside your own jurisdiction or to change the purpose of such transfers should only be done with the approval of the appropriate Data Protection Officer.

Annex C - INFORMATION TECHNOLOGY DEPARTMENT

LAWFUL PURPOSES

New Uses

Use of data for a new purpose, can also affect BRUSCH SERVICES SRL's filings with data protection authorities (e.g. new IT applications or system developments). IT Staff should check that the relevant Department making the request has consulted the Data Protection Officer, if they wish to use personal data for a new purpose.

DATA QUALITY

Test Data

Where live data is used for test purposes (if at all necessary), such data should where possible be anonymized prior to any such testing.

Data Review

Datasets should be reviewed regularly to ensure data is classified in line with Rules on Company information treatment by employees, Information Security Manual as well as to identify duplicate records, synchronize data, simplify access and streamline databases.

SECURITY

The Information Technology Department is responsible for assessing the Information Technology requirements to ensure appropriate security and will consult with the other Departments where appropriate. Much of this detail is set out in the Information Security Manual, Security Incident Management and related policies which should be consulted in addition to this document.

The Information Technology Department is responsible for reclaiming any IT equipment from staff who leave and ensuring that any hard drives are wiped.

The Information Technology Department is responsible for ensuring that all laptops and other portable media are encrypted.

TRANSFERS

Where any system development or change in the IT services is planned (e.g. relocating data centers, changing IT applications or service providers, adopting new IT solutions and technologies) which may result in a transfer of data, you must seek the input of the appropriate Data Protection Officer.

RIGHTS

The Information Technology Department should action any requests from other Departments to update or correct information held in the databases managed by the Information Technology Department (to the extent that the Departments do not have the appropriate editing rights).

ANNEX D: FACILITIES

DATA PROTECTION SAFEGUARDS LAWFUL PURPOSES

Requests to disclose data

If you receive a request to forward personal data to a third party such as the police: you should first check with the Head of Personnel Department if it relates to an employee (current or former) or with the Data

Protection Officer. They will determine if the release of this data would breach data protection legislation.
[India 2 and India 6][Malaysia 3] [South Africa 8]

TRANSPARENCY

If data is collected about employees and / or visitors who access a BRUSCH SERVICES SRL entity's premises (e.g. when using a card system): notice about how BRUSCH SERVICES SRL uses this information should be included in an employee privacy notice. Save for the use of CCTV, it is not necessary to give notice to visitors as long as BRUSCH SERVICES SRL's use of their data is likely to be for expected purposes.

Notice of CCTV use
If you are responsible for monitoring the security of BRUSCH SERVICES SRL's premises by use of CCTV cameras (especially in reception areas and car parks): you will be responsible for ensuring that the CCTV is drawn to the attention of employees, visitors and others who may be recorded by positioning prominent notices wherever the CCTV is used.
Before CCTV is introduced into new areas, you must carry out an impact assessment to ensure that there is a business need for monitoring which justifies its use and to ensure that the monitoring is carried out with the minimum of intrusion, and in accordance with any local law requirements.

Sensitive Personal Data
If a specific investigation by Facilities requires the processing of sensitive personal data (e.g. if an employee is suspected of criminal activities and CCTV is used to watch that specific individual for evidential purposes), you should seek prior approval from the Data Protection Officer.

RETENTION

If CCTV images are stored, this will be for a maximum period of 30 days.
Visitor registers should be destroyed 3 years after the visitor has been to the building.

DATA QUALITY

You should ensure that there is a clear and foreseeable need for information collected about individuals. For example, CCTV should not be focused on other non-BRUSCH SERVICES SRL private property or on public spaces such as streets.

SECURITY

If access to and movement around some of BRUSCH SERVICES SRL's premises is monitored for security purposes: system access should be checked from time to time to ensure that there are no suspicious movements.

All requests from individuals to see their data (e.g. request for CCTV images) should be promptly forwarded to the Personnel Department (for employees) and to the Data Protection Officer in other situations. However, these Departments may require you to provide certain information in response to the requests. It is important that CCTV images are kept in a format that enables them to be provided in response to a request, provided that they have not already been deleted.

COUNTRY APPENDICES:
Country: ROMANIA

1. Details about sickness can be recorded only if needed for compliance with the specific obligations of BRUSCH SERVICES SRL in labor field (e.g., for documenting the employees' absence).

2. Details of criminal offences should not be requested, unless such is legally requested for holding the respective position.

3. You must inform the unsuccessful applicants that you want to keep CVs on file for future use and CVs should only be retained if the applicants give their explicit consent on such.

4. Monitoring of employees' correspondence on a continuous basis (active monitoring) is not allowed. Likewise, monitoring/ processing of employees' e-mails clearly marked as "Private" or monitoring of employees' discussions by telephone or by way of other electronic communications means is strictly forbidden and may qualify as criminal offence.

5. The existence/ using of the CCTV needs to be pointed out by using a pictogram of an appropriate size and placed at a reasonable distance from the place where the CCTV cameras are installed. Generally, the use of CCTV within the area of the offices is strictly forbidden, save for the case where made based on the prior approval of the Romanian supervisory authority. Also, the use of hidden CCTV cameras is not allowed, unless in the limited cases set forth by the law. In no case may CCTV be used in places which, by their nature, impose the preservation of intimacy (e.g. toilettes).