

DATA PRIVACY NOTICE SUMMARY

1. INTRODUCTION

This Data Privacy Notice applies to people who work for us. It explains what personal data we may collect, use, store and transfer; how we may use it; and provides additional information to comply with our obligations under privacy laws. [[click for more detail](#)]

2. RESPONSIBILITY FOR DATA PRIVACY

The data controller for our processing of your personal data is Elavon Financial Services DAC or relevant member of US Bancorp Group identified in your employment contract or contract for services. Other US Bancorp Inc group companies may also be data controllers [[click for more detail](#)].

We have a Data Protection Officer ("DPO") who is responsible for monitoring our compliance with privacy laws. If you have any questions, believe privacy rights have been violated or are concerned there may have been a breach of privacy laws, policies or procedures please contact your local Human Resources contact or the DPO (EUDataProtectionOffice@elavon.com). [[click for more detail](#)]

3. WHAT DATA DO WE PROCESS?

We collect various types of personal data about you including information relating to your personal details, recruitment, screening results, work details, business contact, regulatory and compliance data, pay and benefits, attendance and leave, training and development, performance, disciplinary and grievance and other HR management or business processes, health and safety, working capacity, monitoring data and photographs and other information relating to the administration or management of your employment. [[click for more detail](#)]

We hold some special category data (e.g. health information, race, religion, trade union membership and information relating to criminal records or offences). [[click for more detail](#)]

4. HOW DOES THE COMPANY COLLECT DATA?

We collect your personal data from you. We also obtain information from managers, other departments and occasionally from colleagues. In certain circumstances and in accordance with applicable laws, we obtain some information from third parties (e.g previous employers, regulatory authorities or benefit or other service providers). Lastly, information is also collected through your access and use of certain work areas and systems. [[click for more detail](#)]

5. WHAT ARE THE PURPOSES FOR WHICH DATA ARE PROCESSED AND WHAT LEGAL BASIS APPLIES

We hold and use personal data primarily to ensure that those who work for us are suitable and appropriate and to administer and manage your relationship with us, in line with your contract, our policies and procedures and applicable laws.

We rely on appropriate legal basis whenever we process your personal data. Where processing involves special category data we also rely on an additional legal justification.

Processing will normally be justified because (a) it is necessary to comply with our legal obligations (e.g. employment and health and safety laws, employment equality laws, tax laws or regulatory rules); (b) it is necessary to enter into or comply with your contract (e.g. provide contractual pay and

benefits); or (c) where the processing is necessary for our legitimate interests (or the legitimate interest of a third party) provided, however, this is not overridden by your rights.

The detail of our legitimate interest in particular processing will vary depending on our business purpose. However, in overall terms we have a legitimate interest in attracting and retaining engaged, motivated, high calibre people to work for us; and in securing, defending, managing and developing our business and our people in line with our policies and procedures and in line with our legal and regulatory obligations. Our processing is designed to support these aims. This is important to enable us to deliver our commitments to our customers; to protect our reputation; and to achieve our immediate and longer term business objectives. [[click for more detail](#)]

We will only process special category data where permitted under applicable laws. For example, where necessary to carry out our obligations and / or give effect to your rights in the field of employment, social security and social protection law in line with applicable laws. There are however other grounds we may rely on in some situations. [[click for more detail](#)]

We will only process personal data relating to criminal convictions and offences where authorised by applicable law. [[click for more detail](#)]

6. AUTOMATED DECISION MAKING AND PROFILING

Details of any automated decision making and profiling we use in recruitment or employment are explained here. [[click for more detail](#)].

7. RETENTION OF PERSONAL DATA

We keep different types of personal data for different periods depending on the nature of the information, the purposes we need it for and applicable legal requirements. [[click for more detail](#)]

8. DISCLOSURES OF PERSONAL DATA

Basic information in our global directories is accessible to employees across the US Bancorp Inc group. Other information will be disclosed internally, in certain limited circumstances, on a need to know basis to appropriate members of management, Human Resources or certain staff in other departments (e.g. finance or IT) where it is necessary to administer the working relationship with you or for them to perform their role, for the purposes described in this notice.

Appropriate information will also be disclosed to third parties, who are not part of the US Bancorp Inc group, such as our system providers, benefit providers, third party processors or professional service advisers. We also share information with national or regulatory authorities to comply with our legal and regulatory obligations.

Wherever required under applicable law, we will enter into data processing or similar agreements with third parties with whom we share your data to ensure appropriate protection of your personal data. [[click for more detail](#)].

9. SECURITY OF DATA

We are committed to protecting the security of your personal data. [[click for more detail](#)]

10. INTERNATIONAL TRANSFER OF PERSONAL DATA

As part of an international group of companies with US Bancorp Inc as the ultimate parent company, some of your personal data will be accessible or transferred to countries both within and outside of the

European Union. This includes transfers within our group of companies and transfers to third parties (e.g. service providers or regulators). Where this is the case we ensure safeguards are in place in compliance with applicable laws including standard contractual clauses approved by the European Commission or other relevant supervisory authorities [[click for more detail](#)].

11. YOUR RIGHTS AS A DATA SUBJECT

You have a number of rights in relation to your personal data including the right of access; to ask us to correct inaccurate data; to ask us to restrict or delete data in certain circumstances; to object to particular processing based on legitimate interest grounds; to withdraw consent, in the limited circumstances where we rely on your consent; to ask to transfer your data in certain circumstances; and to complain to the relevant supervisory authority. [[click for more detail](#)]

12. NOTICE OF CHANGES

We will review this Data Privacy Notice from time to time and will change or update it at any time. We will tell you about any changes.

When we undertake certain processing of personal data which are subject to additional Data Privacy Notices, we will bring these to your attention where they engage. [[click for more detail](#)]

DATA PRIVACY NOTICE

1. INTRODUCTION

- 1.1 In this Data Privacy Notice the terms the "**Company**", "**we**", "**us**" and "**our**" are references to Elavon Financial Services DAC (including its branches) and, where relevant, its subsidiaries, its holding companies including the ultimate parent company US Bancorp Inc and other subsidiaries of US Bancorp Inc ("**US Bancorp Group**").[\[click for more detail\]](#)
- 1.2 This Data Privacy Notice applies to all current and former employees, workers, individual contractors, contingent workers, applicants, interview candidates, interns, agency workers, consultants and directors. References to "**staff**" or "**you**" or "**your**" in this Data Privacy Notice are references to all these categories of individual. Where we use the term "employment" in this Data Privacy Notice this includes also other engagements where you work for us but are not an employee.
- 1.3 We hold and process data on all current and former staff, those applying to work for us and third parties whose information you provide to us in connection with the employment or other working relationship (eg next-of-kin, emergency contact information and/or dependents).
- 1.4 We take your data protection rights and our legal obligations seriously. Your personal data will be treated in a secure and confidential manner and only as set out below or otherwise notified to you in writing.
- 1.5 Please read the following carefully to understand our views and practices regarding your personal data and how we treat it. The following Data Privacy Notice describes the categories of personal data we process, how your personal data is collected, processed, used and transferred, for what purposes we process your data and how your privacy is safeguarded in the course of our relationship with you. It is intended to provide you with information about the Company's processing of your personal data under applicable laws. This Data Privacy Notice does not form part of your contract of employment or engagement with us.
- 1.6 If you have any questions about this Data Privacy Notice or would like to access the information it contains in a different format please contact your local Human Resources contact.

2. RESPONSIBILITY FOR DATA PRIVACY

- 2.1 Elavon Financial Services DAC or the relevant member of US Bancorp Group identified in your employment contract or contract for services is the data controller of your personal data.
- 2.2 In addition, where processing of personal data is undertaken by other members of US Bancorp Group for their own independent purposes, these associated companies will sometimes be data controllers of your personal data.
- 2.3 We have a Data Protection Officer ("**DPO**") who is responsible for, among other matters, monitoring Elavon's compliance with data protection law. You can contact the Company's Data Protection Officer securely and confidentially at any time if you have any concerns about the processing of your personal data or any data protection issue. The DPO's contact details are: - Data Protection Officer, Elavon Financial Services DAC, Cherrywood Business Park, Loughlinstown, Dublin 18, D18 W319. Email address: EUDataProtectionOffice@elavon.com

2.4 If you have any questions regarding the processing of your personal data, about your data privacy rights or if you believe your data privacy rights have been violated, please contact your local Human Resources contact or, where applicable, the Data Protection Officer, email address: EUDataProtectionOffice@elavon.com. If you are aware of an unauthorised disclosure of data, please refer to the reporting requirements in the Elavon Financial Services DAC Data Protection Policy.

3. WHAT DATA DO WE PROCESS?

3.1 The Company collects and processes your personal data for the purposes described in this Data Privacy Notice. Personal data means any information describing or relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

3.2 In accordance with and subject to applicable laws, we collect various types of personal data about you for the purposes described in this Data Privacy Notice, which can include:

3.2.1 **Personal details:** your title, name(s), gender, nationality, civil/marital status, date of birth, age, home contact details (eg address, telephone or mobile number, e-mail), previous address, passport or other national ID number, social security number, immigration and eligibility to work information, driving licence, languages spoken; next-of-kin/dependent/emergency contact information (names, surnames, relationship to employee, address, contact number), details of any disability and any adjustments or accommodations required as a result and your biometric data relating to your handprint if you choose to provide that for site entry purposes;

3.2.2 **Recruitment and candidate selection data:** skills and experience, qualifications, references, employment history, academic history, CV and application, record of interview, interview and assessment centre documentation and outcome, outcome of ability tests, outcome of personality profiling, vetting and verification information (eg where permitted by applicable law results of judgements search, financial sanction check, regulatory sanction check and a basic disclosure criminal record check relating to unspent convictions), information related to the outcome of your application, details of any offer made to you;

3.2.3 **Data related to your engagement:** contract of employment or engagement, work contact details (eg corporate address, telephone number, e-mail), employee or payroll number, photograph, work location, default language, time zone and currency, worker and system IDs, work biography, assigned business unit, reporting line, worker category, hire/contract begin and end dates, terms and conditions of engagement, cost centre, job title and job description, working hours and patterns, status (active/inactive/terminated), role change history, trade union membership where relevant and permitted by applicable law;

3.2.4 **In employment screening data:** results of periodic judgements check, global watchlist check, financial sanction check, regulatory sanction check and an employee disclosure criminal record check relating to unspent convictions where relevant and permitted by applicable law to comply with regulatory requirements applicable to Elavon Financial Services DAC and/or US Bancorp Inc;

- 3.2.5 **Regulatory data:** records of your registration with any applicable regulatory authority, regulated status and any regulatory certificates and references;
- 3.2.6 **Remuneration, pension and benefits data:** remuneration information (including salary/rate of pay/fees as applicable, allowances, overtime, bonus and commission plans and related target and achievement data), payments for leave/absence (eg holiday pay, sick pay, family leave pay), bank account details, grade, national insurance or social security number, tax information (e.g. tax authority forms, tax codes), third party benefit recipient information (eg expression of wish and dependents information including names, date of birth and medical history if relevant), benefit details, expenses, deductions, salary sacrifice arrangements, share scheme participation details;
- 3.2.7 **Time, Attendance and Leave data:** timekeeping and attendance records, holiday, leave and absence records (including dates, reasons, requests and approvals), records relating to family leave (e.g. maternity, paternity etc), special leave (eg bereavements, jury service, compassionate) and other paid or unpaid leave;
- 3.2.8 **Absence management data:** absence history, medical notes, details of incapacity, details of work impact and adjustments, Doctor contact details, details of treatment and prognosis, manager and HR communications, return to work interviews, meeting records, medical reports, occupational health reports;
- 3.2.9 **HR processes data:** such as flexible working process records (e.g. requests, consideration and outcomes);
- 3.2.10 **Restructuring, reorganisation and redundancy data:** restructure, reorganisation and redundancy records and outcomes (e.g. change plans, consultation records, selection and redeployment data);
- 3.2.11 **Performance and talent management data:** probationary period review records, performance results, targets and objectives, performance improvement data, colleague and manager feedback, performance and potential assessments, review meeting records, records of retention risk review, succession plans, formal and informal performance management process records;
- 3.2.12 **Training and development data:** data relating to training and development needs or training received or assessments completed, employee career profile;
- 3.2.13 **Disciplinary and grievance data:** allegations, complaints, investigation and proceeding records and outcomes;
- 3.2.14 **Health and safety data:** health and safety audits, health and safety screening requests and results, risk assessments, incident reports;
- 3.2.15 **Monitoring data (to the extent permitted by applicable laws):** closed circuit television footage (CCTV), building access, equipment use, which includes the information systems used, and all content created, accessed, transmitted or stored, such as email, electronic files and internet activity, as well as compliance with policies. Additional information on the Security Monitoring is set out in relevant policies: Information Security Services' [Acceptable Use Policy](#), Information Security Services' [Logging and Monitoring Policy](#) and Payment Card Industry (PCI) Data Security Standard Procedures;

- 3.2.16 **Call and computer screen monitoring data:** recordings of calls and screen activities of customer service employees during interactions with customers via phone;
 - 3.2.17 **Code of Ethics Hotline:** details of issue reported and your awareness or involvement, follow up details and investigation records;
 - 3.2.18 **Termination data:** termination/contract end date, the reason for termination and supporting data, exit interviews, termination or settlement agreement, references to be provided to prospective employers and supporting data;
 - 3.2.19 **Employee claims, complaints and disclosures information:** subject matter of employment or contract based litigation and complaints, pre-claim conciliation, communications, settlement discussions, claim proceeding records, employee involvement in incident reporting and disclosures;
 - 3.2.20 **Equality and diversity data:** where permitted by law and provided voluntarily, (e.g. data regarding gender, age, nationality,). This is de-personalised for equal opportunities monitoring purposes;
 - 3.2.21 **Outsourcing projects and corporate transactions:** data for due diligence process where potential transfer of your employment out of the Company or within the Group;
 - 3.2.22 Any other additional personal data which you choose to provide to the Company or Company personnel during the course of your employment whether verbally or in written form;
 - 3.2.23 Informal opinion data generated in the course of your engagement relating to the administration or management of the Company's relationship with you;
- 3.3 Certain additional information may be collected where this is necessary and permitted by local applicable laws and if this arises we will let you know.

3.4 **Special Category Personal Data**

To the extent permitted by applicable laws the Company will collect and process a limited amount of personal data falling into special categories, sometimes called "sensitive personal data". This term means information relating to:

- 3.4.1 racial or ethnic origin;
- 3.4.2 political opinions;
- 3.4.3 religious or philosophical beliefs;
- 3.4.4 physical or mental health (including details of accommodations or adjustments);
- 3.4.5 trade union membership;
- 3.4.6 sex life or sexual orientation;
- 3.4.7 biometric and genetic data; and
- 3.4.8 criminal records and information regarding criminal offences or proceedings.

4. HOW DOES THE COMPANY COLLECT DATA?

- 4.1 The Company collects and records your personal data from a variety of sources, but mainly directly from you. You will usually provide this information directly to your managers or local Human Resources (HR) contact or enter it into our systems (for example, through your self-service access to our HR systems, your participation in HR processes, emails and instant messages you send or through verbal information which will be recorded electronically or manually). In addition, we collect your personal data from your managers, HR, or occasionally your colleagues (for example, manager feedback and assessment, evidence from colleagues in investigations or peer review exercises).
- 4.2 We will also obtain some information from third parties: for example, references from a previous employer, medical reports from external professionals, information from tax authorities, benefit providers or where we employ a third party to carry out a background check (where permitted by applicable law).
- 4.3 In some circumstances, data will be collected indirectly from monitoring devices or by other means (for example building and location access control and monitoring systems, CCTV, telephone logs and recordings, instant message logs and email and Internet access and use records), if and to the extent permitted by applicable laws. In these circumstances, the data will be collected by the Company or a third party provider of the relevant service.
- 4.4 Where we ask you to provide personal data to us on a mandatory basis, we will inform you of this at the time of collection. Failure to provide certain information will mean that we cannot carry out certain HR processes. For example, if you do not provide us with your bank details, we will not be able to pay you. In some cases, it means that we may be unable to continue with your employment or engagement as the Company will not have the personal data we believe to be necessary for the effective and efficient administration and management of our relationship with you.
- 4.5 Apart from personal data relating to you, you will also provide the Company with personal data of third parties, notably your dependents and other family members, for purposes of HR administration and management, including the administration of benefits and to contact someone in an emergency. Before you provide such third party personal data to the Company you must first inform these third parties of any such data which you intend to provide to the Company and of the processing to be carried out by the Company, as detailed in this Data Privacy Notice.

5. WHAT ARE THE PURPOSES FOR WHICH DATA IS PROCESSED AND WHAT IS OUR LEGAL BASIS FOR CARRYING OUT THE PROCESSING?

5.1 The legal basis on which we process your personal data

5.1.1 Whenever we process your personal data we do so on the basis of a legal basis or justification for that processing. Processing of special categories of data is always justified on the basis of an additional lawful condition. In the majority of cases, the processing of your personal data will be justified on one of the following basis:

5.1.1.1 The processing is necessary for compliance with a legal obligation to which the Company is subject; or

- 5.1.1.2 Where the processing is necessary for the performance of a contract to which you are a party or in order to take steps at your request prior to entering into such a contract; or
- 5.1.1.3 We also process your personal data where the processing is in accordance with legitimate interests pursued by the Company, except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal data. Where we rely on legitimate interests, we have summarised the legitimate interest we rely on in this Data Privacy Notice.
- 5.1.2 If our processing involves the collection or use of special categories of data, where that is permitted under applicable laws, we also rely on an additional legal justification set out below in section 5.3.
- 5.1.3 We will, on occasion, process your personal data for the purpose of legitimate interests pursued by a third party, except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal data (for example to meet the security requirements of our customers).
- 5.1.4 In exceptional circumstances, you may ask us to process data for a particular purpose, we will carry out the processing on your instruction and on your behalf (for example if you ask us to provide pay information to a bank for a mortgage application made by you).
- 5.1.5 We have set out below the purposes we use your personal data for and the legal basis we rely on in each case.

5.2 The purposes we use personal data for and the legal basis that applies

We have identified a number of purposes for collecting and processing your personal data which are subject to applicable data protection laws. These are set out below together with the legal basis we rely on in each case:

No.	Purpose for processing	The lawful basis we rely on and additional detail about our legitimate interest where relevant
a)	<p>Recruitment and selection</p> <p>To assess your suitability to work for us, compare you with other applicants and make a decision whether to offer you employment;</p> <p>To consider any adjustments or accommodations for the recruitment process or if you were to commence work with us in the event you have a disability</p>	<p>Some of this processing is necessary for the compliance with legal obligations to which the Company is subject including the requirement to ensure we do not unlawfully discriminate in our recruitment decision.</p> <p>Some of this processing is necessary for taking steps at your request to enter into a contract with you. Where you have applied to work for us we need to use your personal data to make an offer of employment to you where appropriate.</p> <p>Additional processing is necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in fully assessing applicants to ensure that only suitable and appropriate candidates are selected, to compare candidates and decide who to recruit. The Company aims to recruit the best person</p>

		for each vacancy through fair, systematic, effective recruitment and selection procedures.
b)	<p>Pre-employment screening and verification</p> <p>Pre-employment screening including, where relevant, appropriate and permitted by applicable law: judgements check, global watchlist checks, financial sanction checks, regulatory sanctions check and a basic disclosure check in relation to suspect criminal activities;</p> <p>Verification of your identity, home address, academic and work history and right to work.</p>	<p>This processing is necessary for the compliance with legal obligations to which the Company is subject including establishment of the right to work in the country in which you are employed; and our compliance with regulatory requirements to which Elavon Financial Services DAC as an employer, its European branch entities or US Bancorp must adhere to.</p> <p>Additional screening which is not legally required or referred to above is necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in ensuring that candidates for employment or engagement do not pose an unacceptable risk to the business or its customers and considers the verification carried out necessary to support the Company's and US Bank Corp's regulatory compliance, prevent crime and other unlawful acts and to protect the business and customers from fraud, dishonesty or incompetence.</p>
c)	<p>Job offers - Making job offers and providing contracts of employment</p> <p>On boarding and HR administration - Taking steps to on board you where you accept an offer from us including transferring relevant recruitment information onto employment records and the day to day administration of your employment.</p>	<p>Some of this processing is necessary for the compliance with legal obligations to which the Company is subject including the requirement to issue written particulars or terms of employment and the requirement not to unlawfully discriminate in the terms of any offer to you.</p> <p>Additionally, some of this processing is necessary to take steps to enter into the contract between you and the Company and to perform that contract to make an appropriate offer to you and administer your employment contract if you join us.</p> <p>Other aspects of the processing are necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in ensuring the effective engagement of staff on appropriate terms and conditions of employment, that there is a smooth transition into employment for successful candidates and an effective administration of the employment relationship.</p>
d)	<p>Future job opportunities</p> <p>To contact you if you are not successful should another potentially suitable vacancy arise during the twelve months following completion of the recruitment process for the</p>	<p>This processing is necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in maintaining an appropriate pool of talent who have shown an interest in working for the Company and who are potentially suitable candidates for employment. This will potentially benefit both initially unsuccessful candidates and the Company.</p>

	role you applied for.	
e)	<p>Recruitment queries and challenges</p> <p>To deal with any query, challenge, request for feedback or claim received in relation to our recruitment decisions</p>	<p>This processing is necessary for the compliance with legal obligations to which the Company is subject including ensuring that the Company is able to demonstrate its compliance with data protection laws and employment equality laws.</p> <p>Beyond legal compliance, processing is necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in being able to provide feedback to candidates and to be able to defend any challenge or claim made in connection with our recruitment decision. This will assist the Company to avoid the risk of financial exposure or costs incurred through challenges to recruitment decisions and to maintain its reputation.</p>
f)	<p>Training and development</p> <p>Training, development, promotion, career progression, talent identification and retention, succession planning and business contingency planning.</p>	<p>Processing related to role related training is necessary to perform the contract between you and the Company.</p> <p>The other aspects of processing are necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in managing its workforce and operating its business. This includes ensuring that each employee is trained for their role. It also includes ensuring that there are succession and contingency plans in place so that the business can maintain knowledge, skills and relationships. This also includes supporting and developing our personnel in their career to help the Company retain engaged, motivated, high calibre employees.</p>
g)	<p>Pay and benefits</p> <p>Awarding, providing and administering remuneration, benefits and incentive schemes and reimbursement of business costs and expenses and making appropriate tax and social security deductions and contributions</p>	<p>This processing is necessary for the compliance with legal obligations to which the Company is subject including the provision of statutory payments and benefits and complying with the requirements of the tax authorities in relation to tax and social security.</p> <p>Processing is also necessary to perform the contract between you and the Company in order to provide and administer the payments and benefits we have agreed to provide to you as part of your contract of employment.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in ensuring that remuneration is set an appropriate level and properly administered.</p>
h)	<p>Work management</p> <p>Allocating and managing</p>	<p>Some processing is necessary to perform the contract between you and the Company to ensure that you carry out the role</p>

	<p>duties and responsibilities and the business activities to which they relate, including business travel</p>	<p>under your contract of employment.</p> <p>Additional processing is necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in managing its workforce and business. This includes ensuring the effective allocation and organisation of work amongst its employees and ensuring that each employee carries out appropriate duties.</p> <p>Effective employee management in this way is important to enable the Company to carry out its commitments to customers and to manage its resources efficiently and effectively.</p>
<p>i)</p>	<p>Identification and communication</p> <p>Identifying and communicating effectively with staff;</p> <p>Development and maintenance of US Bancorp Group directories and skills databases</p> <p>We will use photographic images most commonly to identify you and aid communication and collaboration (e.g. on your ID badge or pass, emails, other communications coming from you, internal CVs, for events you attend, or campaigns or projects you are involved with, team lists etc)</p>	<p>Using your data to communicate with you is necessary for the compliance with legal obligations to which the Company is subject including the need to communicate with you regarding processes governed by employment laws (e.g. a consultation exercise or investigation) or as part of our duty of care towards you.</p> <p>Processing is also necessary to perform the contract between you and the Company. Communication is important to operate your contract of employment.</p> <p>Additional processing is necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in managing its workforce and operating its business. This includes effective communication.</p> <p>The Company also has a legitimate interest in contributing to appropriate safety and security by ensuring that employees can be identified.</p> <p>The Company also has a legitimate interest in facilitating effective communication and collaboration between staff and between staff and others to maximise operational performance and collaboration and to help staff work together for the benefit of the business and the Company's customers.</p>
<p>j)</p>	<p>Performance and Talent Reviews</p> <p>Setting performance expectations and objectives, monitoring and measuring performance against goals and objectives, managing and operating performance reviews and career potential</p>	<p>This processing is necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in setting objectives for staff to ensure that members of staff are aligned to the needs and goals of the Company; in measuring the achievement of staff against those objectives; assessing the development needs staff to ensure the highest standards of performance and to support career.</p>

	reviews	The Company has a further legitimate interest in ensuring an appropriate performance related measure to support fair, consistent, objective performance related reward and to support performance assessment for the purpose of other HR processes.
k)	<p>Formal HR Management Procedures</p> <p>Dealing with issues and concerns relating to performance, capability, absence, conduct and employee complaints including informal and formal performance management, disciplinary and grievance related reviews, managing allegations and complaints, investigations and other informal and formal HR processes and making related management decisions</p>	<p>This processing is necessary for the compliance with legal obligations to which the Company is subject, including our duty of care towards you, to avoid unlawful dismissal and comply with employment equality laws.</p> <p>This processing is also necessary to perform the contract between you and the Company where we have committed to comply with certain procedures as part of your terms and conditions of employment.</p> <p>Additional processing is necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in managing its workforce and operating its business. This includes putting in place appropriate standards, policies and procedures for employees and taking action if they are not complied with.</p>
l)	<p>Employee Relations And Engagement</p> <p>Consultations or negotiations with staff or representatives of staff</p> <p>Engagement programmes such as surveys for benchmarking and identifying improved ways of working</p>	<p>This processing is necessary for the compliance with legal obligations to which the Company is subject including statutory consultation or collective bargaining obligations.</p> <p>Processing is also necessary for the purpose of the legitimate interests pursued by the Company where the consultation or employee engagement programme is not a statutory matter. The Company has a legitimate interest in seeking the views of its workforce on business improvement opportunities and on proposals which will impact on staff. Effective employee engagement helps ensure the Company makes the best decisions for the business and is important to attract and retain high calibre employees.</p>
m)	<p>Absence and Incapacity Management</p> <p>Processing information about absence or physical or mental health in order to: assess eligibility for incapacity related remuneration or benefits; determine working capacity; facilitate return to work; make adjustments or accommodations to duties</p>	<p>Some of this processing is necessary for the compliance with legal obligations to which the Company is subject including health and safety laws, our duty of care to staff, , avoiding unlawful dismissal and compliance with disability discrimination laws.</p> <p>Additional processing is necessary to perform the contract between you and the Company including the provision of payments and benefits relating to absence or incapacity.</p> <p>Additional processing is also necessary for the purpose of the legitimate interests pursued by the Company.</p>

	or the workplace; make decisions regarding employment or redeployment.	The Company has a legitimate interest in managing and supporting its workforce and taking steps to identify and mitigate risks to staff health, safety or welfare, ensure fitness for work and to manage absence and incapacity impacting on the ability of staff to perform their roles.
n)	<p>Restructuring, corporate transactions and outsourcing</p> <p>Planning, managing and carrying out restructuring or redundancies or other change programmes, corporate transactions or outsourcing of services.</p>	<p>This processing is necessary for the compliance with employment laws to which the Company is subject including, where relevant, in relation to rules relating to the automatic transfer of staff from one organisation to another; redundancies or potential terminations due to business reasons; and laws regulating corporate transactions.</p> <p>Additional processing beyond legal compliance is necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in planning and implementing changes in its operations to preserve operations, maximise efficiency, grow or modernise its business in a fair and effective way.</p> <p>Business change and transformation is important to ensure business continuity and to support the Company's immediate and long-term business goals and outcomes.</p>
o)	<p>IT Network and system protection and operation of and compliance with Company policies and procedures</p> <p>Including audits and compliance monitoring, access controls and permissions.</p> <p>Including related system maintenance.</p>	<p>This processing is necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in managing its workforce and operating its business and protecting its business and all stakeholders (including customers, employees and shareholders) from various risks.</p> <p>This includes putting in place appropriate standards, policies and procedures for employees, measuring compliance, detecting breaches and taking action if they are not complied.</p> <p>It also includes appropriate protection of the IT network, systems and business devices to maintain the integrity and security of data and business information and facilitating records management.</p> <p>This is important to maintain business standards, ensure business continuity and to protect the Company's operation and reputation.</p> <p>Additional information on Information Security policies is set out in mandatory online training "SAFE – Information Security Awareness" in Global Learning Lab and at [click for more detail]</p>

p)	<p>Customer service call and screen monitoring</p> <p>calls monitoring and computer screen monitoring of customer service employees' interactions with customers is carried out for quality and training purposes</p>	<p>Processing is necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest maximising operational performance, ensuring customer service quality standards are maintained, improving the customer experience and identifying and assessing the training and development needs staff to ensure the highest standards of performance.</p>
q)	<p>Safety and security</p> <p>(including CCTV and access controls);</p>	<p>Processing is necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in ensuring that its business, customers, employees, assets and systems are safe and secure.</p>
r)	<p>Business protection</p>	<p>This processing is necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in ensuring that its business, customers, employees, assets, systems, business relationships and information are protected.</p> <p>This is important to comply with our obligations to our customers and staff to protect their information and assets as well as to protect the Company's business.</p>
s)	<p>Compliance with laws and regulation</p> <p>Complying with laws and regulation applicable to the Company</p> <p>This includes the operation of the ethics hotline to enable staff to raise compliance concerns.</p>	<p>This processing is necessary for the compliance with legal obligations to which the Company is subject (for example maternity or parental leave legislation, working time and health and safety legislation, taxation rules, worker consultation requirements, other employment laws, and financial services and other regulation to which the Company is subject in the conduct of its business)</p> <p>The operation of the ethics hotline is necessary for the purpose of the legitimate interests pursued by the Company. The Company has a legitimate interest in preventing and detecting unlawful acts and regulatory and other compliance concerns in order to protect its business and reputation.</p>
t)	<p>Equality of opportunity monitoring</p> <p>Monitoring programmes to ensure equality of opportunity and diversity with regard to personal characteristics protected under applicable employment equality laws where permitted by</p>	<p>This processing is necessary for the purpose of the legitimate interests pursued by the Company. The Company has a legitimate interest in ensuring that it takes action to prevent discrimination and promote an inclusive and diverse workplace.</p>

	applicable law	
u)	<p>Information Management, business planning and reporting</p>	<p>Some of this processing is necessary for the compliance with legal obligations to which the Company is subject including statutory Company reporting obligations and corporate governance requirements.</p> <p>Additional processing is necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in managing its workforce and operating its business, ensuring appropriate governance and controls are in place and to measure and report on financial management and business performance and plan for the future.</p> <p>This includes appropriate preparation of internal and external reports on a range of business areas. Effective planning, management information and reporting is important for effective management of the business, risk management and decision making.</p>
v)	<p>Business development and customer, supplier and stakeholder liaison</p> <p>For business development purposes</p> <p>For tenders for work or customer team records or to operate the day to day relationship with customers;</p> <p>To operate the relationship with other third parties such as suppliers;</p> <p>This includes the use of photographic images where appropriate</p>	<p>This processing is necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in winning business and growing its business, complying with contracts entered into with customers, ensuring the success of customer relationships and seeking to ensure customer loyalty.</p> <p>This includes the sharing of appropriate information with customers and prospective customers about who is or will be working with them to develop relationships with and support the effective performance of commitments for customers. In some cases this will also include supporting customers to comply with their legal or regulatory obligations or security requirements by having sufficient information about those providing services to them.</p> <p>The Company also has a legitimate interest in ensuring that it can develop and operate the relationship with other trade partners effectively.</p> <p>Supporting successful business relationships is important for business continuity, improvement and growth to help the Company achieve its short and long term goals.</p>
w)	<p>Business communications and media</p> <p>This will sometimes include the use of photographic images where appropriate</p>	<p>This processing is necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in communicating effectively with its workforce, customers, trade partners, other stakeholders and the market and media.</p>

		<p>That includes providing information about relevant business initiatives including identifying those of our staff who are leading the relevant matters being communicated.</p> <p>Effective communication contributes to successful business relationships and maintaining and enhancing the Company's profile and reputation to support business protection, performance and growth.</p>
x)	<p>References</p> <p>Complying with reference requests where the Company is named by the individual as a referee</p>	<p>This processing is necessary for the purpose of the legitimate interests pursued by the Company and potential new employers. It is in the legitimate interests of a new employer to receive confirmation of basic employment details from the Company for the purposes of confirming a former employee's employment history.</p>
y)	<p>Litigation</p> <p>To enforce our legal rights and obligations, and for any purposes in connection with any legal claims made by, against or otherwise involving you</p>	<p>This processing is necessary for the compliance with legal obligations to which the Company is subject including demonstrating compliance with employment and health and safety laws and data protection laws.</p> <p>Additional processing is necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company considers that it has a legitimate interest in protecting its organisation from breaches of legal obligations owed to it and to defend itself from litigation to protect the Company's reputation and to protect the Company from damage or loss.</p>
z)	<p>Disclosure obligations</p> <p>To comply with lawful requests by public authorities (including without limitation to meet national security or law enforcement requirements), discovery requests, or where otherwise required or permitted by applicable laws</p>	<p>This processing is necessary for the compliance with legal obligations to which the Company is subject where there is a legal obligation to disclose information or a court or other legal order to provide information is place.</p> <p>Processing is also necessary for the purpose of the legitimate interests pursued by the Company.</p> <p>The Company has a legitimate interest in co-operating with relevant authorities, government bodies or regulators for the provision of information where appropriate. The Company wishes to maintain its reputation as a good corporate citizen and to act ethically and appropriately in all the countries in which it does business.</p>

5.3 Additional legal basis we rely on where we process special category data

The special categories of personal data that will be processed by the Company are set out above. Where we process special categories of data it will be justified by a condition set out at 5.2 above and also by one of the following additional conditions:

- 5.3.1 The processing is necessary for the purposes of carrying out the obligations and exercising the rights of you or the Company in the field of employment law, social security and social protection law, to the extent permissible under applicable laws;
- 5.3.2 The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of your working capacity, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services, to the extent permitted by applicable laws;
- 5.3.3 The processing is necessary to protect your vital interests or of another person where you are physically or legally incapable of giving consent (for example in exceptional emergency situations, such as a medical emergency);
- 5.3.4 The processing is necessary for purposes in the substantial public interest authorised by applicable law.
- 5.3.5 The processing is necessary for purposes authorised by applicable law, including processing for insurance purposes.
- 5.3.6 The processing is necessary for the establishment, exercise or defence of legal claims; or
- 5.3.7 In exceptional circumstances the processing is carried out subject to your explicit consent (as explained below).

5.4 The purposes we use special category personal data for and the additional legal basis that applies

We have identified a number of purposes for collecting and processing your special category personal data. These are set out below together with the additional legal basis we rely on in each case:

No.	Purpose for processing	Additional lawful basis for special category data processing
a)	Documentation such as work permits, details of residency, proof of citizenship will be processed to assess and review eligibility to work for the Company in the jurisdiction in which you work	This processing is necessary for the purposes of carrying out the obligations and exercising the rights of you or the Company in the field of employment law, social security and social protection law, to the extent permissible under applicable laws. In particular the requirement to check that you are legally permitted to work in your jurisdiction.
b)	Health and medical information will be used to comply with employment, health and safety or social security laws. For example, to carry out statutory risk assessments and regular health and safety assessments, or maternity benefits, avoid	This processing is necessary for the purposes of carrying out the obligations and exercising the rights of you or the Company in the field of employment law, social security and social protection law, to the extent permissible under applicable laws. In particular those laws set out in this section. To the extent that this data is managed by our

	<p>breaching legal duties to you, to ensure fair and lawful management of your employment, avoid unlawful termination of your employment, to administer the Company's private medical and long term disability schemes, to make reasonable accommodations or adjustments and avoid unlawful discrimination or dealing with complaints arising in this regard. It may also be used for insurance purposes.</p>	<p>occupational health advisers, this processing is necessary for the purposes of preventive or occupational medicine, for the assessment of your working capacity, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services, to the extent permitted by applicable laws.</p> <p>Where relevant this data may be used where necessary for insurance purposes.</p>
c)	<p>Details of trade union membership will be processed to ensuring that any relevant rights that you will have in connection with any Trade Union membership are complied with, as required to enable us to meet our obligations under employment law</p>	<p>This processing is necessary for the purposes of carrying out the obligations and exercising the rights of you or the Company in the field of employment law, social security and social protection law, to the extent permissible under applicable laws. In particular human rights laws relating to freedom of association and assembly, laws relating to the Company's interaction with Trade Union members and officials and avoiding detrimental treatment relating to Trade Union membership or activities.</p>
d)	<p>Special category personal data of any type will be used in the management and investigation of any complaint under the code of ethics hotline or the Company's grievance, whistleblowing, anti-bullying and harassment or similar policies and procedures or disciplinary procedures where such information is sufficiently relevant to the particular complaint or issue.</p>	<p>This processing is necessary for the purposes of carrying out the obligations and exercising the rights of you or the Company in the field of employment law, social security and social protection law, to the extent permissible under applicable laws. In particular employment laws relating to the effective management of complaints and avoiding unlawful dismissals, employment equality laws and our duty of care to staff.</p>
e)	<p>If you choose to provide your biometric data relating to your handprint to use the biometric site access we will process this to confirm your identity for security reasons when you use the relevant entrance.</p>	<p>This processing would be based on your consent. If you do not wish to provide this data then you will use the alternative building access that relies on ID card rather than biometric data. The provision and use of this data is therefore optional.</p>

5.5 We may on an exceptional basis seek your consent to certain processing which is not otherwise justified under one of the above basis. If consent is required for the processing in question, it will be sought from you separately. Information regarding such processing will be provided to you at the time that consent is requested, along with the impact of not providing any such consent. It is not a condition or requirement of your employment to agree to any request for consent from the Company.

5.6 Processing data relating to criminal convictions and offences

Personal data relating to criminal convictions and offences will only be processed where authorised by applicable laws. For example:

5.6.1 Criminal records or information relating to criminal offences or convictions may be processed on recruitment or transfer or intermittently where ongoing screening is required where authorised by applicable laws including, subject to local laws:

5.6.1.1 where necessary and proportionate for the performance of your contract or to take steps at your request to enter into a contract with you; or

5.6.1.2 where otherwise authorised by law where necessary for us to comply with our regulatory requirements.

5.6.2 An allegation of a criminal offence or conviction arising during your relationship with the Company will be processed where required or authorised by applicable law. For example:

5.6.2.1 where we have a legal or regulatory requirement to report an offence; or

5.6.2.2 where necessary for the purpose of complying with or assisting other persons to comply with a regulatory requirement (e.g. Central Bank of Ireland requirements) which involves taking steps to establish whether another person has committed an unlawful act or been involved in dishonesty, malpractice or other seriously improper conduct

5.6.2.3 applicable laws authorise the Company to process information about the offence (e.g. in a disciplinary process) for the purpose of performing your contract and making decisions regarding your relationship with the Company.

5.7 Additional information to ensure transparency for particular processing

5.7.1 Additional information regarding specific processing of personal data will be notified to you locally or as set out in applicable policies. This additional information is to ensure you have access to full details of the relevant data and purposes it is used for where it would be disproportionate to set that out in this Data Privacy Notice and it is not obvious. For example:

5.7.1.1 Additional details regarding the type of data collected and monitored within **Information Security monitoring** and how it is used will be found in the Information Security Services' [Logging and Monitoring Policy](#);

5.7.1.2 Physical security monitoring is conducted for security purposes only. Additional details regarding the type of data collected and monitored regarding **Physical Security monitoring** and how it is used can be found in the PCI Physical Security – Section 9 of [Payment Card Industry Data Security Standard Procedures](#);

5.7.2 It will normally be relatively obvious from the relevant HR process or the information set out in this Data Privacy Notice how your personal data will be used. However, there will be occasions where personal data is collected or processed for a number of purposes which will not be obvious. Where we believe this is the case we will aim to make this clear to you. Examples (where permitted by applicable law) include:

5.7.2.1 Personal data primarily relating to any purpose will, if sufficiently relevant and where the circumstances warrant it, be used in a formal investigation such as a disciplinary or grievance investigation e.g training or system access records;

5.7.2.2 Unspent disciplinary or performance sanctions will be taken into account in career progression or restructuring selection decisions;

5.7.2.3 Internal CVs, performance review/appraisal data and talent review data will be taken into account in assessing potential for promotion, succession planning, merit pay increases, bonus awards and restructuring selection decisions;

5.7.2.4 Attendance data will be taken into consideration in relation to merit bonus awards (subject to adjustments or accommodations in relation to disability).

6. AUTOMATED DECISION MAKING AND PROFILING

6.1 We do not currently use automated decision making in the context of recruitment or the employment relationship.

6.2 We do from time to time carry out limited personality, emotional intelligence and career potential profiling both on recruitment and during the employment relationship. Where carried out this is used for development or for consideration in recruitment, career progression, promotion and succession planning. It will not however be used as the sole basis for any decision impacting you.

7. RETENTION OF PERSONAL DATA

7.1 The Company endeavours to ensure that personal data are kept as current as possible and that irrelevant or excessive data are deleted or made anonymous as soon as reasonably practicable.

7.2 The Company's general approach is to only retain personal data for as long as is required to satisfy the purpose for which it was collected by us or provided by you. This will usually be the period of your employment/contract with us plus the length of any applicable statutory limitation period following your departure, although some data, such as pension information, will need to be kept for longer and some information will be deleted earlier. We will keep some specific types of data, for example, tax records, for different periods of time, as required by applicable law. However, some personal data will be retained for varying time periods in

order to comply with legal and regulatory obligations and for other legitimate business reasons.

8. DISCLOSURES OF PERSONAL DATA

- 8.1 Within the Company, your personal data can be accessed by or will be disclosed internally on a need-to-know basis to:
 - 8.1.1 local, regional and where appropriate global Human Resources, including managers and team members;
 - 8.1.2 local, regional and executive management responsible for managing or making decisions in connection with your relationship with the Company or when involved in an HR process concerning your relationship with the Company (including, without limitation, staff from Compliance, Legal, Employee Relations and Information Security);
 - 8.1.3 system administrators; and
 - 8.1.4 where necessary for the performance of specific tasks or system maintenance by staff in the Company teams such as the Finance and IT Department and the HR information systems support teams.
- 8.2 Certain basic personal data, such as your name, location, job title, contact information, employee number and any published skills and experience profile will also be accessible to other employees.
- 8.3 Your personal data will also be accessed where appropriate by third parties whom we work together with (including without limitation Workday, ServiceNow, HireRight, PeopleSoft, PeopleFluent, ADP, Global Learning Lab and their associated companies and sub-contractors) for providing us with services, such as hosting, supporting and maintaining the framework of our HR information systems or the provision of advice or employee benefits. These providers will change from time to time.
- 8.4 Personal data will also be shared with certain interconnecting systems such as local payroll and benefits systems. Data contained in such systems will be accessible by providers of those systems, their associated companies and sub-contractors.
- 8.5 Examples of third parties with whom your data will be shared where appropriate include tax and social security authorities, regulatory authorities, the Company's insurers, bankers, IT administrators, lawyers, HR consulting services providers, marketing and event services providers, auditors, investors, health and safety consultants, occupational health providers and other professional advisors, payroll providers, and providers and administrators of the Company's benefits programs and third party staff vetting providers and your doctor or medical advisers where we will be seeking a report. The Company expects such third parties to process any data disclosed to them in accordance with applicable law, including with respect to data confidentiality and security.
- 8.6 Where these third parties act as a "data processor" (for example a payroll provider or our HR system provider Workday) they carry out their tasks on our behalf and upon our instructions for the above mentioned purposes. In this case your personal data will only be disclosed to these parties to the extent necessary to provide the required services. We will enter into a data processing or similar agreement with such third parties ensuring appropriate protection for

your personal data. Under such agreements, we will be liable for the onward transfer of your personal data.

- 8.7 In addition, we will share personal data with national authorities in order to comply with a legal obligation to which we are subject. This is for example the case in the framework of imminent or pending legal proceedings or a statutory audit.

9. SECURITY OF DATA

- 9.1 The Company is committed to protecting the security of the personal data you share with us. In support of this commitment, we have implemented appropriate technical, physical and organisational measures to ensure a level of security appropriate to the risk. The Company uses a variety of technical and organisational methods to secure your personal data in accordance with applicable laws.

- 9.2 A number of the measures that we use to protect information are set out in Elavon Financial Services DAC Data Protection Policy and the Information Security Services' Acceptable Use Policy which sets out the applicable Company policies. The company is PCI DSS (Payment Card Industry Data Security Standard) and ISO27001 certified. In addition, our security practices follow the NIST cybersecurity framework.

- 9.3 If you are in possession of personal data of any kind (eg data collected in emails, address books, Excel spreadsheets, CVs or other records) you must ensure that the data are kept in a safe place where unauthorised access cannot occur and in line with the Company's policies and procedures. You must comply with the security obligations contained in the Company's policies or procedures communicated to you.

- 9.4 You should not create, copy or export personal data relating to any other person outside of official company storage locations and systems except where necessary for a specific authorised and lawful purpose under this Data Privacy Notice. In this event appropriate measures must be taken to protect the confidentiality and integrity of the data during the processing. Once the relevant processing is complete, steps should be taken to store or return the relevant data within the official storage locations/systems with all less formally held records (e.g. local folders, hard copies, emails saved outside of formal managed folders) securely erased.

10. INTERNATIONAL TRANSFER OF PERSONAL DATA

- 10.1 Your personal data (including special categories of personal data) will be transferred to associated companies of the Company to process for the purposes described in this Data Privacy Notice. This will be applicable for example where the relevant company or a manager from that company is responsible for conducting or approving the relevant process or the data is part of a global directory where other individuals need to have access.

- 10.2 These associated companies or managers will be located within the European Union and elsewhere in the world (for example [[click for more detail](#)]).

- 10.3 Personal data will also be transferred to third parties (e.g. service providers or regulators as set out above), who will have systems or suppliers located outside the European Union (for example Workday, PeopleSoft and Global Learning Lab both host data in the United States of America).

- 10.4 As a result, your personal data will be transferred to countries outside of the country in which you work or outside of the European Union to countries whose data protection laws will be less stringent than yours.
- 10.5 The Company will ensure that appropriate or suitable safeguards are in place to protect your personal information and that transfer of your personal information is in compliance with applicable data protection laws.
- 10.6 Where required by applicable data protection laws, the Company has ensured that service providers (including other Company associated companies) sign standard contractual clauses as approved by the European Commission or other supervisory authority with jurisdiction over the relevant Company exporter. You can obtain a copy of any standard contractual clauses in place which relate to transfers of your personal data by contacting EUDataProtectionOffice@elavon.com.
- 10.7 The Company has an intra-group data transfer agreement in place which regulates cross-border transfers of your data within the Group.
- 10.8 You have a right to request a copy of any data transfer agreement under which your personal data is transferred, or to otherwise have access to the safeguards used. Any data transfer agreement made available to you will be redacted for reasons of commercial sensitivity.

11. YOUR RIGHTS AS A DATA SUBJECT

11.1 Right to access, correct and delete your personal data

- 11.1.1 The Company aims to ensure that all personal data are correct. You also have a responsibility to ensure that changes in personal circumstances (for example, change of address and bank accounts) are notified to the Company so that we can ensure that your data is up-to-date.
- 11.1.2 You have the right to request access to any of your personal data that the Company will hold, and to request correction of any inaccurate data relating to you. You furthermore have the right to request deletion of any irrelevant data we hold about you.
- 11.1.3 You can see and update some of this data such as Emergency Contacts or Phone Numbers yourself via Workday. However, to correct/update any information used for payroll and employment purposes, you will need to contact local Human Resources contact.

11.2 Data portability

Where we are relying upon your consent or the fact that the processing is necessary for the performance of a contract to which you are party as the legal basis for processing, and that personal data is processed by automatic means, you have the right to receive all such personal data which you have provided to the Company in a structured, commonly used and machine-readable format, and also to require us to transmit it to another controller where this is technically feasible.

11.3 Right to restriction of processing:

You have the right to restrict our processing of your personal data where:

- 11.3.1 you contest the accuracy of the personal data until we have taken sufficient steps to correct or verify its accuracy;
- 11.3.2 where the processing is unlawful but you do not want us to erase the data;
- 11.3.3 where we no longer need the personal data for the purposes of the processing, but you require them for the establishment, exercise or defence of legal claims; or
- 11.3.4 where you have objected to processing justified on legitimate interest grounds (see below) pending verification as to whether the Company has compelling legitimate grounds to continue processing.

Where personal data is subjected to restriction in this way we will only process it with your consent or for the establishment, exercise or defence of legal claims.

11.4 Right to withdraw consent

Where we have relied on your consent to process particular information and you have provided us with your consent to process data, you have the right to withdraw such consent at any time. You can do this by (i) in some cases deleting the relevant data from the relevant HR system (although note that in this case it will remain in back-ups and linked systems until it is deleted in accordance with our data retention policy) or (ii) contacting your local Human Resources contact. It will only however be rarely that we rely on your consent to process personal data for your employment or engagement.

11.5 Right to object to processing justified on legitimate interest grounds

Where we are relying upon legitimate interest to process data, then you have the right to object to that processing. If you object, we must stop that processing unless we can either demonstrate compelling legitimate grounds for the processing that override your interests, rights and freedoms or where we need to process the data for the establishment, exercise or defence of legal claims. Where we rely upon legitimate interest as a basis for processing we believe that we can demonstrate such compelling legitimate grounds, but we will consider each case on an individual basis.

11.6 Right to complain

You also have the right to lodge a complaint with a supervisory authority if you consider that the processing of your personal data infringes applicable law (see www.dataprotection.ie).

- 11.7 For further information regarding your rights, or to exercise any of your rights, please contact: Data Protection Officer, Elavon Financial Services DAC, Cherrywood Business Park, Loughlinstown, Dublin 18, D18 W319. Email address: EUDataProtectionOffice@elavon.com

12. NOTICE OF CHANGES

- 12.1 The Company will change or update this Data Privacy Notice at any time.
- 12.2 Should we change our approach to data protection, you will be informed of these changes or made aware that we have updated the Data Privacy Notice so that you know which information we process and how we use this information.
- 12.3 This Data Privacy Notice was last updated and reviewed on 10th December 2020.

APPENDIX – US BANCORP INC ENTITIES

In this Data Privacy Notice the terms the "**Company**", "**we**", "**us**" and "**our**" are references to Elavon Financial Services DAC (including its branches) and, where relevant, its subsidiaries, its holding companies including the ultimate parent company US Bancorp Inc and other subsidiaries of US Bancorp Inc ("US Bancorp Group"), including:

Elavon Financial Services DAC, a company registered in Ireland under Company Registration No. 418442 whose registered address is Block E, First Floor, Cherrywood Business Park, Loughlinstown, Co. Dublin, Ireland and its branches operating in the EEA under the same entity name including:

United Kingdom Branch (company number BR022122 whose registered office is at 2nd Floor, 70-Gracechurch Street, London, EC3V 0HR);

Spain Branch (tax identification number W-00718181 whose registered office is at Avenida de Bruselas, 36, 28108, Alcobendas, Madrid, Spain);

Norway Branch (company registration number 991 283 900 whose registered office is at Karenslyst Alle 11, 0278, Oslo, Norway);

Germany Branch (company number 45766660 whose registered office is at Lyoner Strasse 36, Frankfurt am Main 60528, Germany);

Poland Branch (company number 287836 whose registered office is at ul. Pulawska 17, 02-515, Warszawa, Poland);

Belgium Branch (company number 0829.613.086 whose registered office is at Pegasus Park, De Kleetlaan 5B-5C, 1831 Diegem, Belgium);

Luxembourg Branch (registration number B244276; whose registered office is at: Floor 3, K2 Ballade, 4, rue Albert Borschette, L-1246 Luxembourg);

U.S. Bank Global Corporate Trust Limited, a company registered in the UK (company number 05521133 whose registered address is 125 Old Broad Street, Fifth Floor, London EC2N 1AR);

U.S. Bank Global Fund Services Ireland (company number 413707 whose registered address is 24 – 26 City Quay, Dublin 2, Ireland, D02 NY19);

U.S. Bank Global Fund Services Luxembourg (company number B238278; whose registered address is at: Floor 3, K2 Ballade, 4, rue Albert Borschette, L-1246 Luxembourg);

Elavon, Inc., Two Concourse Parkway, Suite 800, Atlanta, GA 30328, U.S.A., Tel: 1-678-731-5000; **U.S. Bancorp**, U.S. Bank Place, 601 Second Avenue South, Minneapolis, Minnesota 55402-4302, U.S.A., Tel: 1-651-466-3000.

Elavon Digital Europe Limited (company number 07492608, whose registered office is: Second Floor, Q16, Quorum Business Park, Benton Lane, Newcastle Upon Tyne, England, NE12 8BX);

Elavon Digital Dublin Limited (company number 87704, whose registered office is: Building 8 Cherrywood Business Park Loughlinstown Dublin 18, Ireland);

Talech Lithuania, UAB (company registration code 305153437, whose registered address is Ašigalio g. 1b, Kaunas, Lietuvos Respublika, Office location: Laisvės al. 82, Kaunas);

Norse Nordic AB (company number 559201-3113, whose registered office is at Stora Ävägen 21, 436 34 Askim, Sweden).