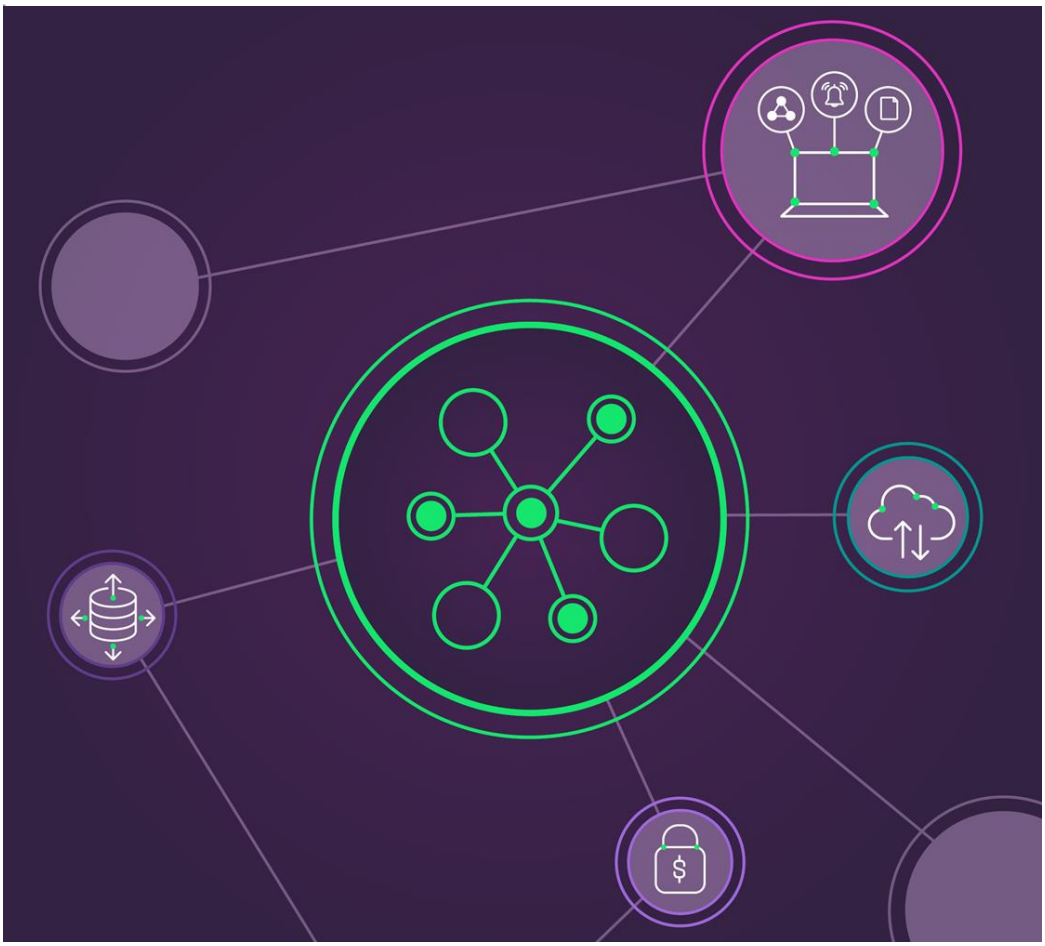


Data Protection & Privacy Policy

BS ISO/IEC 27001:2013

Date: August 2022
Version: 3.1
CONFIDENTIAL

Contents

1. Introduction 2
2. Interpretation 3
3. Scope and Importance 5
4. Personal Data Protection Principles 6
   - 4.1. Lawfulness, Fairness and Transparency 7
   - 4.2. Consent 7
   - 4.3. Transparency (Notifying Data Subjects) 8
   - 4.4. Purpose Limitation 8
   - 4.5. Data Minimisation 8
   - 4.6. Accuracy 9
   - 4.7. Storage Limitation 9
   - 4.8. Security Integrity and Confidentiality 9
     - 4.8.1. Protecting Personal Data 9
   - 4.9. Reporting a Personal Data Breach 10
   - 4.10. Transfer Limitation 10
   - 4.11. Data Subject's Rights and Requests 11
   - 4.12. Accountability 12
5. Record Keeping 12
6. Training and Audit 13
7. Privacy by Design and Data Protection Impact Assessment (DPIA) 13
8. Automated Processing (Including Profiling) and Automated Decision-Making 14
9. Direct Marketing 14
10. Sharing Personal Data 15
11. Document Control 15

1. Introduction

The protection of Personal Data is of paramount importance to Quantexa and our customers.

This **Data Protection And Privacy Policy** (the "**Policy**") sets out how **Quantexa Limited**, a company registered in England (10045407), with its principal place of business at WeWork, 10 York Rd, Lambeth, London SE1 7ND and all affiliated companies of the Quantexa Group ("**we**", "**our**", "**us**", "**Quantexa**") handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

This Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This Policy applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Policy when Processing Personal Data on our behalf and attend training on its requirements. This Policy sets out what we expect from you for Quantexa to comply with applicable law. Your compliance with this Policy is mandatory.

Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Policy and are referred to herein. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this Policy may result in disciplinary action.

Local country addendums with respect to applicable national Data Protection Law shall be issued to accompany this Policy and should be reviewed as notified to you.

Where you have a specific responsibility in connection with Processing such as capturing Consent, reporting a Personal Data Breach, conducting a DPIA as referenced in this Policy or otherwise then you must comply with the Related Policies and Privacy Guidelines.

This Policy (together with Related Policies and Privacy Guidelines) is an internal document and should not be shared with third parties, clients or regulators without prior authorisation from the Quantexa Data Protection Officer ("**DPO**").

The policy will be reviewed annually by the Quantexa Data Protection Officer, or within planned and agreed intervals, to determine whether it has achieved its intended outcome(s) over the past year, to review the objectives going forward and to identify opportunities for continual improvement.

This Policy does not override any applicable national data privacy laws and regulations in countries where Quantexa operates.

If you have any questions with respect to this Policy or the protection of Personal Data, at any time – please contact the DPO – Guy Muir; guymuir@quantexa.com.

2. Interpretation

Definitions:
In this Policy the following terms shall have the meaning as set out below. Additional definitions may be set out in the applicable Country Addendum:

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

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

Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, members and others of the Quantexa Group , as applicable.

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

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Country Addendum: means the applicable additional or supplementary requirements and conditions under a relevant Data Protection Law in a territory where Quantexa operates (e.g. Australia).

Criminal Record Data: means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings. This includes any information which is in the public domain such as a news report on a convicted criminal.

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

Data Protection Law: the applicable laws to the processing of Personal Data by Quantexa which may include:

- UK Data Protection Act 2018;
- EU General Data Protection Regulation ((EU) 2016/679);
- Privacy Act 1988 (Cth) (Australia);
- Canadian Personal Information Protection and Electronic Documents Act 2004 (PIPEDA);
- California Consumer Privacy Act of 2018 (CCPA);
- Colorado Privacy Act;

- Personal Data Protection Act 2012 (Singapore).

and all other applicable laws with respect to the business operations of Quantexa as applicable and updated from time to time.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the UK GDPR.

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

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

EU General Data Protection Regulation (GDPR): the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

UK GDPR: the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) as defined in the Data Protection Act 2018. Personal Data is subject to the legal safeguards specified in the UK GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data as set out in further detail below, but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

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

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with Data Protection Law .

Privacy Guidelines: Quantexa privacy and related guidelines are provided to assist in interpreting and implementing this Policy and Related Policies as set out in the Schedules or links in this Policy, are available on the Quantexa's Data Privacy section of the Policy Centre and on the Legal SharePoint page.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when Quantexa collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for

example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

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

Quantexa Group: includes the Quantexa Limited, Quantexa Inc., Quantexa BVBA, Quantexa Canada Limited, Quantexa Pte. Ltd and Quantexa Pty. Ltd.

Related Policies: Quantexa's policies, operating procedures or processes related to this Policy and designed to protect Personal Data, are available on the Quantexa Data Privacy Page and on the Legal SharePoint page or as otherwise made known to you where applicable.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. Quantexa will treat these types of data as if they are Special Categories of Personal Data:

3. Scope and Importance

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. Quantexa is exposed to potential fines including under the GDPR of up to EUR20 million (£17.5 million) or 4% of our total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the UK GDPR.

All of the Quantexa Group personnel are responsible for ensuring that they comply with this Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.

The DPO is responsible for overseeing this Policy and, as applicable, developing Related Policies and Privacy Guidelines.

The Quantexa DPO is:

Guy Muir

General Counsel

E: guymuir@quantexa.com

T: +44(0) 7467 825 048

Please contact the DPO with any questions about the operation of this Policy or Data Protection Law or if you have any concerns that this Policy is not being or has not been followed.

In particular, you must always contact the DPO in the following circumstances:

a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by Quantexa) (see section 4.1);
b) if you need to rely on Consent and/or need to capture Explicit Consent (see section 4.2);
c) if you need to draft Privacy Notices (see section 4.3);
d) if you are unsure about the retention period for the Personal Data being Processed (see section 4.4);
e) if you are unsure about what security or other measures you need to implement to protect Personal Data (see section 4.5);
f) if there has been a Personal Data Breach (section 4.9);
g) if you are unsure on what basis to transfer Personal Data outside the EEA (see section 4.10);
h) if you need any assistance dealing with any rights invoked by a Data Subject (see section 4.11);
i) whenever you are engaging in a significant new, or change in Processing activity which is likely to require a DPIA (see section 7) or plan to use Personal Data for purposes other than what it was collected for;
j) if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see section 8);
k) if you need help complying with applicable law when carrying out direct marketing activities (see section 9); or
l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see section 10).

4. Personal Data Protection Principles

We adhere to the principles relating to Processing of Personal Data including those set out in the GDPR which require Personal Data to be:

a) processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);
b) collected only for specified, explicit and legitimate purposes (Purpose Limitation);
c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);
d) accurate and where necessary kept up-to-date (Accuracy);
e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);
f) processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);

g) not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and

h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

4.1. Lawfulness, Fairness and Transparency

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The UK GDPR allows Processing for specific purposes, some of which are set out below:

a) the Data Subject has given his or her Consent;

b) the Processing is necessary for the performance of a contract with the Data Subject;

c) to meet our legal compliance obligations;

d) to protect the Data Subject's vital interests;

e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests needs to be set out in applicable Privacy Notices.

You must identify and document the legal ground being relied on for each Processing activity in accordance with Quantexa's guidelines on Lawful Basis for Processing Personal Data.

Please note with respect to Criminal Records Data very strict conditions apply to any collection or processing of Criminal Record Data. Any proposed processing of Criminal Record Data must be approved by the DPO. If you have any questions or concerns as to whether Criminal Record Data may potentially be processed contact the DPO.

4.2. Consent

A Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

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

When processing Special Category Data or Criminal Record Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents in accordance with Related Policies and Privacy Guidelines so that Quantexa can demonstrate compliance with Consent requirements.

4.3. Transparency (Notifying Data Subjects)

The UK GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. The information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects we shall provide the Data Subject with all the information required by the UK GDPR including the identity of the Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the applicable Data Protection Law and on a basis which contemplates our proposed Processing of that Personal Data.

If you are collecting Personal Data from Data Subjects, directly or indirectly, then you must provide Data Subjects with a Privacy Notice in accordance with our Related Policies and Privacy Guidelines.

4.4. Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

4.5. Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with Quantexa's data retention guidelines.

4.6. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

4.7. Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

Quantexa will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires that data to be kept for a minimum time.

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

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all Quantexa's applicable records retention schedules and policies. This includes requiring third parties to delete that data where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

4.8. Security Integrity and Confidentiality

4.8.1. Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate

security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data.

You must exercise particular care in protecting Special Categories of Personal Data and Criminal Record Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

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

You must comply with all applicable aspects of our Information Security Policies, further details of which can be found in the Information Security section of the Policy Centre, and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the relevant standards to protect Personal Data.

4.9. Reporting a Personal Data Breach

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

The UK GDPR requires Controllers to notify any Personal Data Breach to the applicable regulator (in the UK it will be the Information Commissioner) and, in certain instances, the Data Subject **within 72 hours.**

Individual customers of Quantexa may have a shorter period in which to report such a breach and must should be carefully assessed

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO as set out above or any member of the Quantexa Management Team who will follow the Quantexa Information Security Management Plan.

4.10. Transfer Limitation

The UK GDPR restricts data transfers to countries outside the EEA to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

Quantexa transfers Personal Data originating in one country across borders when we transmit, send, view or access that data in or to a different country. This will include viewing data on a screen outside the EEA even if no data is physically sent.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

Other applicable Data Protection Law and individual customer contracts of Quantexa may have additional restrictions on transferring data to a third country which should be carefully assessed.

4.11. Data Subject's Rights and Requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

a) withdraw Consent to Processing at any time;

b) receive certain information about the Data Controller's Processing activities;

c) request access to their Personal Data that we hold;

d) prevent our use of their Personal Data for direct marketing purposes;

e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

f) restrict Processing in specific circumstances;

g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

i) object to decisions based solely on Automated Processing, including profiling (ADM);

j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

l) make a complaint to the supervisory authority;

m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format; and

Quantexa must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

If you receive or are unsure as to the receipt of a Data Subject request, you must immediately forward any Data Subject request you receive to HR, your line manager or the DPO.

4.12. Accountability

The Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

Quantexa must have adequate resources and controls in place to ensure and to document compliance including:

a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;
b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
c) integrating data protection into internal documents including this Policy, Related Policies, Privacy Guidelines or Privacy Notices;
d) regularly training Company Personnel on Data Protection Law, this Policy, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. Quantexa must maintain a record of training attendance by Company Personnel; and
e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

5. Record Keeping

The UK GDPR requires us to keep full and accurate records of all our data Processing activities.

You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with Quantexa's record-keeping guidelines.

These records should include, at a minimum:

a) the name and contact details of the Controller and the DPO; and clear descriptions of:
b) the Personal Data types;
c) the Data Subject types;
d) the Processing activities;
e) the Processing purposes;
f) the third-party recipients of the Personal Data;
g) the Personal Data storage locations;
h) the Personal Data transfers;
i) the Personal Data's retention period; and
j) a description of the security measures in place.

To create the records, data maps should be created which should include the detail set out above together with appropriate data flows.

6. Training and Audit

We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training in accordance with Quantexa's mandatory training guidelines.

You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

7. Privacy by Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

You must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that Process Personal Data by taking into account the following:

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

Data controllers must also conduct DPIAs in respect to high-risk Processing.

You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated Processing including profiling and ADM;
- large-scale Processing of Special Categories of Personal Data or Criminal Record Data; and
- large-scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

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

8. Automated Processing (Including Profiling) and Automated Decision-Making

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

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

If certain types of Special Categories of Personal Data or Criminal Record Data are being processed, then grounds (b) or (c) will not be allowed but the Special Categories of Personal Data and Criminal Record Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

Where you are involved in any data Processing activity that involves profiling or ADM, you must contact the DPO for approval.

9. Direct Marketing

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt-in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

10. Sharing Personal Data

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers, if:

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

11. Document Control

Author	Guy Muir	
Role	DPO/General Counsel	
Version	3.1	
Creation Date	August 2022	
Next Review	May 2023	
Classification	Quantexa Confidential	
Revision notes	Update to include references to local country addendums and increased Data Protection Law.	
Approvals		
Name	**Role**	**Date**

Guy Muir	General Counsel & DPO	17/08/2022
Ray O'Brien	COO	23/08/2022