Privacy Policy – Xapo Bank (Gibraltar) Limited

Last Updated: March 17th, 2020

Introduction

Xapo Bank (Gibraltar) Limited (“Xapo Bank”) respects your privacy and is committed to protecting your Personal Data. This Privacy Policy applies to how we collect, process, and store your Personal Data through our online services, our Android and iOS Mobile apps, recipients of our emails, or when you otherwise interact with us. This Privacy Policy describes the types of Personal Data we obtain, how we use the Personal Data, and with whom we share it. We also describe your rights, how the law protects you, and how you can contact us about our privacy practices.

If you are submitting information through our recruitment solution linked to this website, please read carefully our separate Job Applicant Privacy Notice

This privacy policy is provided in a layered format so you can click through to the specific areas set out below.

IMPORTANT INFORMATION AND WHO WE ARE

Purpose Of This Privacy Policy

This Privacy Policy aims to give you information on how Xapo Bank collects and processes your Personal Data.

It is important that you read this Privacy Policy together with any other privacy policy or fair processing policy we may provide on specific occasions when we are collecting or processing Personal Data about you so that you are fully aware of how and why we are using your Personal Data.

This Privacy Policy is supplemented by other privacy policies or notices and is not intended to override them.

In this Policy, “Xapo”, "we", "us" and "our" refers to Xapo Bank.

In this Privacy Policy, “Personal Data” means any information relating to you as an identified or identifiable natural person (“Data Subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an online identifier or to one or more factors specific to your physical, physiological, genetic, mental, economic, cultural or social identity.

For the avoidance of doubt, Personal Data does not include data from which you cannot be identified (which is referred to simply as data, non-Personal Data, anonymous data, or de-identified data).

In this Privacy Policy, “processing” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Identity and the Contact Details of the Controller

For the purposes of the General Data Protection Regulation (“GDPR”) Xapo Bank is the data controller and responsible for the Personal Data that we collect or that you provide to us.

If you have any questions or comments about this Privacy Policy or any issue relating to how we collect, use, or disclose Personal Data, or if you would like us to update information we have about you, or more general queries you can contact us at: support@xapo.com

You can also contact us in writing at:

- Full name of legal entity: Xapo Bank (Gibraltar) Limited, a ‘credit institution’ regulated by the Gibraltar Financial Services Commission under the Financial Services Act 2019 with permission number 23171.

- Postal address: Xapo Bank. Unit 1.02, First Floor, World Trade Center, 6 Bayside Road, Gibraltar, GX11 1AA.

Or by phone on our telephone number: +350 2000 8125

Contact Details of the Data Protection Officer

We have appointed a Data Protection Officer who is responsible for overseeing questions in relation to this privacy policy and to inform you how to exercise your rights. Our Data Protection Officer can be contacted directly at: dpo@xapo.com

2. THE DATA WE COLLECT ABOUT YOU AND HOW WE USE IT

We will only use your Personal Data when the law allows us to. Most commonly, we will use your Personal Data under the following circumstances:

Consent

When you give us your consent, for example, to access your contacts on your phone or allow us to have access to your location. You have the right to withdraw your consent at any time. To withdraw your consent just go to the Privacy Settings in our Android or iOS Mobile app or contact us at support@xapo.com

Contract

When we need to execute a contract you have entered into with us by accepting our Terms of Service or specific related terms of services relating to other services offered by us.

Where we need to collect Personal Data under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform our services under the contract we have or are trying to enter into with you (for example, to provide you with any of our services). In this case, we may have to cancel a service you have with us but we will notify you if this is the case at the time.

Legal or regulatory obligation

When we need to collect Personal Data by law. If you fail to provide that data when requested, we will not be able to perform our services under the contract with you (for example, to provide you with any of our products or services). In this case, we will have to cancel a product or service you have with us and we will notify you at that time.

Legitimate Interests

Legitimate Interest means the broader stake that Xapo has in the processing or the benefit that we derive from the processing of your Personal Data.

Where we rely on legitimate interests, we make sure that we consider and balance any potential impact on you and your rights before we process your Personal Data for our legitimate interests.

Additionally, we may also process certain special categories of data such as criminal convictions and biometric data where we are lawfully permitted to do so and only for limited purposes such as fraud or money laundering/terrorist financing prevention and detection. Apart from this, we do not collect any of the following Special Categories of Personal Data about you that includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic data

We also collect, use and share **Aggregated Data** such as statistical or demographic data for any purpose. Aggregated Data could be derived from your Personal Data but is not considered Personal Data in law as this data will **not** directly or indirectly reveal your identity. For example,

we may aggregate your Usage Data to calculate the percentage of users accessing a specific website or Mobile App feature. However, if we combine or connect Aggregated Data with your Personal Data so that it can directly or indirectly identify you, we treat the combined data as Personal Data, which will be used in accordance with this Privacy Policy.

Purposes and Legal Basis for which we will use your Personal Data

We have set out in a table format, a description of all the ways we plan to use your Personal Data, and the legal basis we rely on to do so. We have also identified what our legitimate interests are where appropriate. Note that we may process your Personal Data for multiple legal reasons.

Marketing

We are committed to providing you with choices regarding certain Personal Data uses, particularly around marketing and advertising. We will get your consent before sending third party direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us.

Promotional Offers From Us

We may use your identity, contact, technical, usage and profile data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which services and offers may be relevant for you (we call this marketing).

You can expect to receive marketing communications from us if you have requested information or purchased services from us and you have not opted out of receiving that marketing.

Change of purpose

We will only use your Personal Data for the purposes for which we collected it. We will delete it after fulfilling the intended purpose or after expiration of the respective storage periods.

3. DATA PROCESSING IN OUR PORTFOLIO OF SERVICES

Pay a Contact. People Nearby

The “Pay a Contact” feature is available to you within our App. You can pay anybody who has a Xapo account from your account. When a payment is initiated only the sender and the recipient sees each other’s names, email or phone number, reference text and transaction amount.

“People Nearby” is a feature that allows registered Xapo users, as independent third parties, to contact other registered Xapo users to add or withdraw funds from their Xapo Account by

exchanging funds directly between themselves, subject to the terms, conditions, rates and payment methods agreed directly between the registered Xapo users agreeing to conclude such a transaction.

You can also send money in real time to your contacts, who are also Xapo users, from your mobile phone. To enable this, Xapo will access the contacts stored on your end device if you previously consent to this. You will also only be visible for other customers of Xapo if you have previously expressly consented to this. You can always revoke your consent to be seen as a Xapo user by going into your privacy settings and disable the option of visibility. If you (and the recipient) have the relevant settings in our app activated, we'll use your address book on your phone so you can easily make payments to your contacts who are Xapo users and also receive payments from them.

4. HOW YOUR PERSONAL DATA IS COLLECTED

Information That You Provide to Us

Personal Data that you provide directly to us should be apparent from the context in which you provide it, for example: when you use our services, we must collect your name, email address, and transaction information to complete your transactions. We will process Personal Data that you choose to provide to us through the Website and Mobile Apps, including, but not limited to, your first and last name, physical address, email address, mobile device identifier, or transactional data (e.g., amount of funds associated with a transaction, the type of transaction executed, financial institutions, account information).

Information That We Collect Automatically

We use Personal Data that we collect automatically through cookies and action tags. We also use the information to help diagnose technical and service problems, administer the Site, and identify visitors to the Site.

Cookies: We use cookies on our website to collect data about your visit (like usage data, and other information automatically collected from your browser or mobile device; this information may include your IP address; browser type and version; preferred language; geographic location using IP address or the GPS, wireless, or Bluetooth technology on your device; operating system and computer platform) and to allow you to navigate from page to page without having to re-login each time, count visits, and see which areas and features of our website are popular.

Action Tags: We may use action tags to identify some of the pages that you visit and how you use the content on those pages. Action tags collect and transmit this data in a manner that identifies you if you have registered with our website, and are logged into our online services,

our Android or iOS Mobile apps. We also may use action tags in our emails, to determine whether an email was opened or whether it was forwarded to someone else. When you use our Android or iOS Mobile apps, we may use action tags where you are accessing websites from links in our Android or iOS Mobile apps. These may identify the pages that you visit and how you use the content on those pages.

To learn more about the cookies that we use on our online services, our Android and iOS Mobile apps, as well as to control your cookie settings, please read our Cookie Policy.

We use third party analysis tools to collect data about your computer and internet connection. That information includes, but is not limited to, the IP address of your computer and/or internet service provider, geolocation, when you access our online services, our Android or iOS Mobile apps, the Internet address of websites from which you link to our online services and from which you came to before landing on our online services, the browser that you are using and your movements on our online services. All of this information is used internally for the purposes of understanding how our online services are being used and to improve them. We also use the data collected via cookies to track the popularity of our online services.

We also use third party analysis tools to collect data about your use of our Android and iOS Mobile apps. The information collected identifies the types and timing of actions you take within our Android and iOS Mobile apps, including installation, registration, uploading, and certain types of navigating. All of this information is used internally for the purpose of understanding how our Android and iOS Mobile apps are being used and improving them. Clicking on those links or enabling those connections allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. We accept no responsibility for the actions of these third-party websites. When you leave our online services, we encourage you to read the privacy statements of every Website you visit.

Your browser settings may allow you to transmit a “Do Not Track” signal to websites and online services you visit. Like many other websites and online services, we do not currently process or respond to “Do Not Track” signals from your browser or to other mechanisms that enable choice. If we do so in the future, we will describe how we do so in this Privacy Policy.

Information That We Obtain From Third Parties and Publicly Available Sources

Please find a description in a table format of the information obtained from third parties.

Third Party Links

In addition, please note that this website and our Android and iOS Mobile apps may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our online services or Android and iOS Mobile apps, we encourage you to read the privacy policy of

every webpage or app you visit. We are not responsible for the security of any data you are transmitting over the Internet, or any data you are storing, posting, or providing directly to a third party's website, which is governed by that party's policies. If you have further questions about security, you can contact us using the details provided above.

5. ANTI MONEY LAUNDERING AND COMBATING TERRORIST FINANCING

Money laundering is defined as the process where the sources of funds are disguised so that it gives an impression of legitimate income. Criminals specifically target financial services firms through which they attempt to launder criminal proceeds without the firms' knowledge or suspicion.

Please find out how we will process your Personal Data for these purposes.

6. INFORMATION WE SHARE; DATA TRANSFERS

We do not sell or otherwise disclose Personal Data that you provide to us or that we collect on this website, our online services, or our Android and iOS Mobile apps, except as described here:

- Companies in the Xapo group where it is necessary for the performance of a contract and these entities are used by us to assist in the provision of our services to you. Companies in the Xapo group will be acting as joint controllers in order to provide our services;

- Marketing materials if you have provided consent;

- If required, professional advisers such as lawyers, banks, auditors and insurers providing such services;

- Regulators and other authorities who require reporting of processing activities under certain circumstances;

- If required, or where we believe it is required by applicable laws or legal process;

- To protect the rights, property and safety of Xapo Bank, our users and the public, including, for example, in connection with court proceedings, to detect or prevent criminal activity, fraud, material misrepresentation, or to establish our rights or defend against legal actions;

- Other Xapo Bank users you may interact with through our services, including your public profile which may provide, among others, an avatar selected by you, general information

about you such as your name and surname, broad location, user rating, and the date upon which you a Xapo Bank user only if you have provided consent.

Xapo Bank is headquartered in Gibraltar. However, due to the nature of our global offering, we have operations throughout the world, including but not limited to, North America, South America and Asia. We transfer your data to countries outside the European Economic Area ("third countries") to the extent that is necessary in order to perform our services requested by you.

Whenever we transfer your Personal Data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- Where we use certain service providers, we will use contract language approved by the European Commission which gives Personal Data the same protection it has in Europe.
- Where we use providers based in the US, we will transfer data to them if they are part of the Privacy Shield or Standard Contractual Clauses which requires them to provide similar protection to Personal Data shared between Europe and the US.

Further details on these provisions can be obtained by contacting at support@xapo.com

The Categories of Providers Table provides information on the type of third party recipient (i.e. by reference to the activities it carries out), the industry and the location of the recipients.

7. SECURITY MEASURES

We have put in place appropriate security measures to prevent your Personal Data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We have taken precautions to ensure the security of your data. The Personal Data you have entered on HTML pages (contact forms) and that is stored by us, shall be transmitted to Xapo in encrypted form (TLS - Transport Layer Security) via the public data network, and stored and processed at Xapo.

In addition, we limit access to your Personal Data to those employees, agents, contractors and other third parties strictly needed under the provisions made within a service agreement signed with them. They will only process your Personal Data on our instructions and they are subject to a duty of confidentiality and a duty to comply with data protection procedures.

We have put in place procedures to deal with any suspected or actual Personal Data breach. We will notify you and any applicable authority of a Personal Data breach where we are legally required to do so.

8. PROTECTION OF MINORS

Xapo Bank does not knowingly collect or solicit Personal Data from anyone under the age of 18. If you are under 18, please do not attempt to register for our services or send any Personal Data about yourself to us.

9. DATA RETENTION

We retain information about you in our databases for as long as your account is active, or as is reasonably needed to fulfil the purposes we collected it for and to provide our services, and as required by applicable laws. Our retention and use of your information will be as necessary to comply with our legal, regulatory, tax, accounting, or reporting obligations and requirements, to resolve dispute, or complaints, and to enforce our agreements.

While retention requirements vary by jurisdiction, please find a full description in a table format of all the general retention periods of your Personal Data and the specific legal basis we must comply with. We have also identified what our legitimate interests are where appropriate. Note that we may retain your Personal Data for more than one lawful basis depending on the specific purpose for which we are using your data. Although the table provides our general retention periods stipulated for different categories of Personal Data and/or different processing purposes, in certain circumstances, your information may be retained for longer periods due to the inherent nature of distributed ledger technology.

In some circumstances we will anonymize your Personal Data (so that it can no longer be associated with you) for research or statistical purposes. When information is anonymized, it ceases to be Personal Data and we may use it without further notice to you.

10. YOUR RIGHTS AND CHOICES

Right to Information and access

You have a right to be informed about the processing of your Personal Data. Whilst this Privacy Policy intends to provide you with this information, you can contact us using the details contained in this Privacy Policy to request any further information to access your Personal Data.

Right to rectification

You have the right to have any inaccurate Personal Data about you rectified and to have any incomplete Personal Data about you completed.

The accuracy of your information is important to us. If you do not want us to use your Personal Data in the manner set out in this Privacy Policy, or need to advise us of any changes to your Personal Data, or would like any more information about the way in which we collect and use your Personal Data, please contact us using the details found below.

Right to erasure (right to be 'forgotten')

You have the general right to request the erasure of your Personal Data in the following circumstances:

· the Personal Data is no longer necessary for the purpose for which it was collected;
· you withdraw your consent to processing and no other legal justification for processing applies;
· We unlawfully processed your Personal Data; and
· erasure is required to comply with a legal obligation that applies to us.

We will proceed to comply with an erasure request without undue delay and to such extent we are able to do so, unless continued retention is necessary for:

· Exercising the right of freedom of expression and information;
· Complying with a legal obligation under EU or other applicable law;
· The establishment, exercise, or defense of legal claims.

However, when interacting with the blockchain we may not be able to ensure that your Personal Data is deleted.

Right to restrict processing

You have a right to request to restrict processing of your Personal Data, such as where:

· you contest the accuracy of the Personal Data;
· if you believe processing is unlawful, you may request, instead of requesting erasure, that we restrict the use of unlawfully processed Personal Data;
· we no longer need to process your Personal Data but need to retain your information for the establishment, exercise, or defense of legal claims or regulatory requirements.

Right to data portability

Where the legal basis for our processing is your consent, or the processing is necessary for the performance of a contract to which you are party of, or in order to take steps at your request prior to entering into a contract, you have a right to receive the Personal Data you provided to us in a structured, commonly used and machine-readable format.

Right to object to direct marketing ('opting out')

You have a choice about whether or not you wish to receive information from us.

We will not contact you for marketing purposes unless:

- you have an existing business relationship with us to offer you similar services, and we rely on our legitimate interests as the lawful basis for processing;
- you have otherwise given your prior consent

On each and every marketing communication, we will always provide an option for you to exercise your right to object to the processing of your Personal Data for marketing purposes (known as 'opting-out') by clicking on the 'unsubscribe' button on our marketing emails or choosing a similar opt-out option on any forms we use to collect your Personal Data.

Please note that any administrative or service-related communications (to offer our services, or notify you of an update to this Privacy Policy or applicable terms of service, etc.) will solely be directed at our clients or business partners, and such communications generally do not offer an option to unsubscribe, as they are necessary to provide the services requested.

Therefore, please be aware that your ability to opt-out from receiving marketing and promotional materials does not change our right to contact you regarding your use of our online services and Android or iOS Mobile apps or as part of a contractual relationship we may have with you.

Right to request access

You also have a right to access information we hold about you. We will endeavor to provide you with details of your Personal Data that we hold or process. To protect your Personal Data, we follow established disclosure procedures, which means that we will require proof of identity from you prior to providing such information. You can exercise this right at any time by contacting us using the details found below.

Right to withdraw consent

Where the legal basis for processing your Personal Data is your consent, you have the right to withdraw that consent at any time by contacting us using the details found below.

You can exercise any of the above rights free of charge by contacting us at support@xapo.com

Most of the above rights are subject to limitations and exceptions. We will provide reasons if we are unable to comply with any request for the exercise of your rights.

Right to lodge a complaint with a relevant supervisory authority

If we have not responded to you within a reasonable time or if you feel that your complaint has not been resolved to your satisfaction, without prejudice to any other administrative or judicial remedy, you are entitled to make a complaint to the Information Commissioner under the Gibraltar Data Protection Act 2004 (i.e. the Chief Executive Officer of the Gibraltar Regulatory Authority), which is presently the Gibraltar Regulatory Authority (GRA). You may contact the GRA on the below details:

Gibraltar Information Commissioner
Gibraltar Regulatory Authority
2nd Floor, Eurotowers 4
1 Europort Road
Gibraltar

Email: info@gra.gi
Phone: (+350) 200 74636
Fax: (+350) 200 72166

We would, however, appreciate the chance to deal with your concerns before you approach the Gibraltar Regulatory Authority so please contact us in the first instance at support@xapo.com or dpo@xapo.com

You also have the right to lodge a complaint with the supervisory authority in the country of your legal residence, place of work, or the place where you allege an infringement of one or more of our rights has taken place, if that is based in the European Economic Area.

11. UPDATES ON OUR ONLINE PRIVACY POLICY

We keep our Privacy Policy under regular review and we will update it to reflect any changes.

Changes to this privacy notice may become necessary as we develop our online services, Android and iOS Mobile apps, in order to implement new legal requirements or new technologies and in order to improve the services we provide. If we change our Privacy Policy in the future, we will post the revised version on our website www.xapo.com together with the version number and date of change. You should check this Privacy Policy from time to time when you visit our website.

It is important that the Personal Data we hold about you is accurate and current. Please keep us informed if your Personal Data changes during your relationship with us.

Job Applicant Privacy Notice

What Is The Purpose Of This Document?

The purpose of this privacy notice is to inform you as to, because you are applying to work with us (whether as an employee, worker, consultant or contractor), how and why your personal data will be used, namely for the purposes of the recruitment exercise, as well as how long it will usually be retained for. It provides you with certain information that must be provided under the EU General Data Protection Regulation (EU 2016/26790) ("GDPR")

Xapo Bank is committed to protecting the privacy and security of your personal information.

Xapo Bank is considered a "data controller" and can be contacted at support@xapo.com. This means that we are responsible for deciding how we hold and use personal information about you.

We have appointed a Data Protection Officer ("DPO") who is responsible for overseeing questions in relation to this privacy notice. The DPO will monitor our compliance with legal requirements and with this privacy notice.

Our Data Protection Officer can be contacted directly at: dpo@xapo.com

Data Protection Principles

We will comply with data protection law and principles, which means that your data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

The Kind Of Information We Hold About You

In connection with your application to work with us, we will collect, store, and use the following categories of personal information about you:

- The information you provide to us through our recruitment solution ("Solution") powered by Bamboohr.
- The information you provide to us in your curriculum vitae (solicited or unsolicited) and covering letter and any other submission requested or provided.

- The information you have provided including name; title; address; telephone number; personal email address; phone; employment history; professional achievements and qualifications.

- The application forms; results of post-offer; results of background investigations, related correspondence; certificates of good conduct, interview notes; assessment(s) or skills and behavior assessment test results and references.

- Xapo Bank reserves the right to make an offer of employment subject to the interview due to be held, your previous professional experience, the skills and behaviour test results, your non criminal certificate (if applicable) and references provided.

- We never collect, store and use racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation from applicants in any stage of your interview process.

How Is Your Personal Information Collected?

We collect personal information about candidates from the following sources:

- You, the candidate.

- Your named referees, from whom we collect the following categories of data whether by email or phone call to assess the following non subjective and measurable parameters: Position Held, Reporting Authority and Length of Service.

How we will use information about you

We will use the personal information we collect about you to:

- establish a relationship between a Xapo entity and a potential employee.

- process applications for employment.

- carry out background and reference checks once a decision has been made by us.

- communicate at any stage with you about the recruitment process.

- for such other purposes as permitted by applicable law or with an informed and explicit consent.

Having received your information through the Solution your resume and covering letter or your application form and or the recruitment agency (if any) that provided it to us, after informing you on the hiring process and how we manage your data, we will then process that information to decide whether you meet the basic requirements to be shortlisted for the role or not. If you do, we will decide whether your application is strong enough to invite you for an interview. If we decide to call you for an online or offline interview, we will use the information you provide to us at the interview to decide whether to offer you the role. If we decide to offer you the role, we will then take up references and carry out a skills and behavior assessment test before confirming your appointment.

If You Fail To Provide Personal Information

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully.

Information About Backgrounds

We envisage that we will process and store information about background investigations and certificates of good conduct issued by policing authorities and due diligence of all candidates. Once a decision has been made regarding interest in hiring an applicant any offer will be made contingent upon satisfactory completion of reference checks and criminal background checks.

We will only process information about criminal records, convictions and offences where we have obtained your explicit consent, where necessary for the purposes of performing or exercising our or your obligations or rights under applicable laws and regulations and where it is necessary for the prevention and detection of an unlawful act or for reasons of substantial public interest.

Where we are processing personal information based on your consent, you have the right to withdraw that consent at any time where there is no other legal basis for the processing, by contacting us at jobs@xapo.com

Automated Decision-Making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making.

Data Sharing

Why Might You Share My Personal Information With Third Parties?

We will only share your personal information with selected third parties for the purposes of payroll processing once you become a Xapo consultant, contractor or employee depending on where you are due to be based, whether in Gibraltar, the United States or elsewhere.

All these partners have been required to take appropriate security measures to protect your personal information in line with our policies. We do not allow any third party practice to use your personal data for

their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions**.**

Data Security

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors, consultants and other third parties who have a business need-to-know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained by contacting us at support@xapo.com

Data Retention

How Long Will You Use My Information For?

Type of data	Retention Period	Reference of Justification to retain related data
Employment Records - All Non-Hired Applicants (including all application forms, if any, CVs (which includes contact details) whether solicited or unsolicited; results of post-offer; results of background investigations, if any; related correspondence; certificates of good conduct, if any; interview notes, if any; assessment(s) or psychological test results, if any; references, if any)	12 months from the date of decision not to hire communicated to prospective employees.	To show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way, for up to 12 months since your application is unsuccessful.

Candidates´ Talent Pool

To create a talent pool of potential candidates, Xapo may keep your personal data on file in case there are future employment opportunities with us for which you may be suited for another 12 months. We will ask for your consent before Xapo keeps your data for this purpose and you are free to withdraw your consent at any time by contacting us at jobs@xapo.com

After this period, we will securely destroy your personal information in accordance with our Xapo Data Retention Policy.

Your Rights In Connection With Personal Information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is not a sufficient reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- **Object to the processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information after 12 months from the date of decision not to hire you, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact us at jobs@xapo.com

Right To Withdraw Consent

When you apply for a role, you provide consent to us processing your personal information for the purposes of the recruitment exercise. You have the right to withdraw your consent for processing for that purpose at any time. To withdraw your consent, please contact the person who interviewed you. Once we have received notification that you have withdrawn your consent, we will no longer process your application and, subject to our retention policy, we will dispose of your personal data securely.

Right To Lodge A Complaint

You have the right to make a complaint at any time to the with the data protection authority in the Member State of your habitual residence, place of work, or place of an alleged infringement of the regulation or the Gibraltar Regulatory Authority here once you approached us at dpo@xapo.com with no satisfactory results.

Lawfulness for collection of your personal data

Type of Data	Purpose/Activity	Lawful basis for processing including basis of legitimate interest.
Submitted information: Full name Avatar User identification Address Proof of Address Country of Residence	To verify your identity and liveness, to comply with financial crime, and anti-money laundering/combating the financing of terrorism laws, protect against fraud, and to confirm your eligibility to use our services.	A legal obligation and our legitimate interest, such as the prevention of fraud, misuse of services, or money laundering Fulfilling contracts

Email address Phone number Liveness Selfie Date of Birth	To notify you about changes to our service and privacy policy.	Our legitimate interest, such as to be efficient about how we meet our obligations and comply with regulations that apply to us.
	To comply with a model of automatic exchange of financial account information between tax authorities.*	A legal obligation to cooperate with tax authorities.
	To carry out our contractual obligations arising from any transactions that you conduct.	Our legitimate interest, such as to add extra functions in order to provide a better experience.
	To provide you with information updates about our services.	Fulfilling contracts
<u>User content:</u> ● Customer Service communications and recommendations. ● Names, addresses, email addresses, and telephone numbers of your contacts from your Address Book. ● Ratings and other content that you provide or that is provided about you.	To carry out our contractual obligations arising from any transactions and to enable you to use the "Split a Bill" feature with your contacts who are also Xapo users and any placement of buy or sell bitcoin orders	Fulfilling contracts
	To provide a homogenous experience for users on the platform.	In our legitimate interest to provide other Xapo users with an overview of your trustworthiness when interacting with other Xapo users on social features such as "People Nearby".
	To facilitate real time social interactions through our app.	Your consent.
<u>Transactional Data</u> Transaction Amount Xapo Internal Originator Data Xapo Internal Approver Data Account Number Beneficiary Data User ID or Account/Routing Number Destination User or Institution BTC Receiving Address	To carry out our contractual obligations arising from any financial transactions.	Fulfilling contracts
	To comply with financial crime and anti-money laundering/combating the financing of terrorism laws.	A legal obligation and our legitimate interest, such as the prevention of fraud and money laundering and the performance of a task carried out in the public interest.
	To comply with a model of automatic exchange of financial account information between tax authorities.	A legal obligation to cooperate with tax authorities.
<u>Device information</u>:		

Browser type and version Time zone setting IP address Operating system Type of mobile Unique device identifier	To verify your identity, comply with financial crime laws, tax laws, protect against fraud and to confirm your eligibility.	A legal obligation
	To administer, improve and secure our Xapo site and App for internal operations.	Our legitimate interest to provide and improve our products and services, including our Apps and this Site.
Geolocation information: Information that identifies with reasonable specificity your location by using, for instance, longitude and latitude coordinates obtained through GPS, Wi-Fi, etc.	To maintain your eligibility as a Xapo user. **	Fulfilling contracts
	To simplify the verification of your registered address during the onboarding process. **	Our legitimate interest to improve our customers' experience.
	To verify users' location while using our services to combat financial fraud or other fraudulent use of services **	Our legitimate interest, such as the prevention of fraud, other fraudulent use or misuse of services.
	To provide you with location-specific options, functionality, search results, or other location-specific content.	Your consent and our legitimate interest to improve our visitor guidance experience and supply a value-added service to users.
Statistical information: ● Full uniform resource locators (URL) ● Length of visits to certain pages ● Clickstream to, through, and from our site (including date and time) ● Page response times ● Download reports ● Page interaction information ● Services you viewed or searched for	To administer, improve and secure our Xapo Site and App for internal operations. To provide you with information about other goods and services.	Our legitimate interest, such as being efficient about how we develop new products and services or enhance existing services and keep you updated.

* The automatic exchange of financial account information between tax authorities shall apply to all our customers, excluding the Xapo customers only making use of our "E-Money" services unless informed otherwise. Nonetheless, all of our customers, including those only making use of our "E-Money" services are subject to applicable laws and regulations which may require us to disclose their information where we are legally required to do so.

.** The GPS Location data processing by Xapo shall be mandatory for these purposes or activities for all our customers, excluding the Xapo users only making use of our "E Money" services unless informed otherwise.

Lawfulness for processing of your personal data

People Nearby Data: ● Avatar ● Location	To be visible for other users of Xapo for the purposes of payments between Xapo customers	Your consent

---

Data Obtained from Third Parties

Category of Data Providers	Type of Data that we get	Country of Establishment
Analytics providers, advertising networks, search information providers	Technical Data	USA
Technical, payment and delivery services providers	Contact, Financial and Transaction Data	USA
Data brokers or aggregators	Identity and Contact Data	USA
Publicly available sources [such as Companies House and the Electoral Register]	Identity and Contact Data	EU/EEA

AML KYC Privacy Notice

We will process your identifying data and profile data within operations such as identification (Know your Customer, also known as KYC) and profiling (Customer Due Diligence, also known as CDD) for the purposes of the execution of our Anti Money Laundering (also known as AML) and Counter Terrorism Financing (also known as CTF) customer identification and verification process obligations.

When Xapo asks for CDD, what this refers to is proof of address and proof of identification. This along with information gathered at the application stage paints a picture of any customer (KYC). Without KYC, Xapo may unknowingly become involved with illicit activities and therefore subject to reputational, operational and legal risks, which can result in significant financial cost, or eventual winding up of the institution. KYC is most closely associated with the fight against money-laundering.

Specific proof of address, proof of Identification, source of funds and/or AML-CTF questionnaires that aimed at to fulfil KYC and CDD obligations are compulsory to Xapo users and the failure to be replied might lead (in extreme cases) in the blocking of their accounts or the refusal of services.

In response to the scale and effect of money laundering, the European Union has passed Directives designed to combat money laundering and terrorism. These Directives, together with national regulations as read below, form the cornerstone of our AML/CTF obligations, establish the legal basis for us to process this data and outline the offenses and penalties for failing to comply.

- Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market;
- Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing;
- Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (2000/642/JHA);
- Crime Proceeds of Crime Act 2015;
- Terrorism Act 2018;
- Drug Trafficking Offences Act 1995;

Anti-Money Laundering (AML) Policies

Our AML policy is designed to prevent money laundering by meeting the European standards on combating money laundering and terrorism financing, including the need to have adequate systems and controls in place to mitigate the risk of the firm being used to facilitate financial crime. Our AML policy sets out the minimum standards which must be complied with and includes:

- Appointing a Money Laundering Reporting Officer (MLRO) who has a sufficient level of seniority and independence, and who has responsibility for oversight of compliance with the relevant legislation, regulations, rules and industry guidance;
- Establishing and maintaining a Risk-Based Approach (RBA) to the assessment and management of money laundering and terrorist financing risks faced by the firm. The requirement to provide CDD related data throughout an RBA that will always take into account different factors such as the status of the client, the nature of the transactions, the financial product or the financial flows involved;
- Establishing and maintaining risk-based Customer Due Diligence (CDD), identification, verification and Know Your Customer (KYC) procedures, including enhanced due diligence for customers presenting a higher risk, such as Politically Exposed Persons (PEPs);

- Establishing and maintaining risk-based systems and procedures for the monitoring of on-going customer activity;
- Establishing procedures for reporting suspicious activity internally and to the relevant law enforcement authorities as appropriate;
- Maintaining appropriate records for the minimum prescribed periods;
- Providing training for and raising awareness among all relevant employees.

As a regulated financial institution, Xapo has specific requirements regarding AML systems and procedures. This reflects senior management's desire to prevent money laundering.

Sanctions Policy

Xapo is prohibited from transacting with individuals, companies and countries that are on prescribed sanctions lists. Xapo will therefore screen against United Nations, European Union, UK Treasury and US Office of Foreign Assets Control (OFAC) sanctions lists in all jurisdictions in which we operate.

Automated Decision Making

We do not utilize fully automated decision making processes. We use semi-automated processes which includes, but is not limited to, screening Know-Your-Customer (KYC) and Anti-Money Laundering (AML) data you provide to us in order to assess whether or not we are legally able to allow you to use our services.

All automated screenings are manually reviewed by Xapo compliance analysts. The analyst will review the triage cases to determine if they should be cleared or escalated to the MLRO.

Third Parties AML-KYC

Where processing of personal data is carried out on behalf of Xapo by a third party provider, we conclude a separate contract with the processor with respect to this processing. This contract ensures compliance with European data protection regulations and defines sufficient guarantees for the implementation of appropriate technical and organisational measures, which ensure the protection of your rights.

Categories of Providers

Category of Providers	Service Description	Jurisdictions of Establishment
Infrastructure	Cloud computing	USA

Legal	Consulting such a Lawyers, auditors. Public bodies in connection with court proceedings, to detect or prevent criminal activity, fraud, material misrepresentation, or to establish our rights or defend against legal actions.	USA EU/EEA
Finance	Accountancy, Insurers, Banking institutions and Payment services.	USA EU/EEA
Human Resources	Human resources software as a service.	USA
Product	Document sharing.	USA
Compliance	Clients or institutional on-boarding enhanced due diligence services and know your customers providers, scan and verification passport and ids of users software providers, (KYC) database querying service, Identity Verification for Due Diligence and Know Your Customer requirements. Regulators and other authorities who require reporting of processing activities in certain circumstances.	USA EU/EEA
Customer Care	CRM, FAQ system content provider.	USA

Retention Period Table

Type of data	Retention Period	Reference of Justification to retain related data
Details of third party service providers: ● Name ● Address (previous and new) ● Bank details.	6 years from date of expiration/termination of the contract unless renewed in which case consideration should be given as to whether all contracts should be retained for the duration of the renewal.	For contractual requirements. Defending/Establishing of potential contractual legal claim(s). Limitation Act 1960
Details of suppliers including: ● Email ● Name ● Address ● Bank details.	6 years from date of expiration/termination of the contract unless renewed in which case consideration should be given as to whether all contracts should be retained for the duration of the renewal	Being able to settle Supplier invoices and pay for services provided Defending/Establishing of potential contractual legal claim(s) (Limitation Act 1960)
Suspicious transactions/activities Reports	Upon expiration of purpose or AML/CFT record retention requirement of 5 years minimum under AML and GN or expiration of relationship plus limitation period 6 years under Limitation Act 1960 unless fraud exception	To comply with our AML/CFT and KYC obligations Proceeds of Crime Act 2015 Crimes Act 2011 Financial Services (electronic money) Regulations 2011

● Clients´ Full name ● National ID (includes evidence) ● Address (includes evidence) ● Data of birth ● Phone number ● Email address ● Bank info ● Security selfies ● IP ● OS ● Location ● System ● Time, date and duration of the visit (if stored) ● KYC Data (Blockchain) ● Wallet addresses or other data which could be used to identify the client from data on the blockchain (eg. nonces which could be used to identify hashed data).	Upon expiration of relationship or regulatory requirement for retention (post termination of relationship) minimum of 5 years.	To comply with our AML/CFT and KYC obligations.
Data collected as part of website(s) account creation process / app / platform usage and data relating to users dealings on the website.	Upon the client terminating their account save for any data such as transaction data which may need retained for the end of financial year of 6 years. Maximum of 5 years in case of KYC and AML/CFT ongoing monitoring.	For contractual requirements. Specific legal obligation to retain under the Income Tax Act 2010. KYC/DD obligations under AML/CFT legislation (Proceeds of Crime Act 2015).