Data Protection, Privacy, and Transparency Policy

Jonathan Haywood • VASP (CVC Exchange) • 20 September 2022 • Version 1.0

1. Interpretation

This is the Data Protection, Privacy, and Transparency Policy adopted by Jonathan Haywood in accordance with the Isle of Man Government's "**Data Protection Law - 2018**", the EU's General Data Protection Regulations ("**GDPR**"), and closely aligned with other Isle of Man, EU, UK, and industry-specific legislation, regulations, rules, recommendations, and guidance.

Several legal instruments constitute the Isle of Man Government's "Data Protection Law - 2018":

- The Data Protection Act 2018
- The Data Protection (Application of the GDPR) Order 2018
- The adapted text of the EU GDPR in the Annex to the GDPR Order
- The Data Protection (Application of the LED) Order 2018
- The GDPR and LED Implementing Regulations 2018

All information about my customers is referred to as "**personal data**". The collecting, storing, recording, and use of such personal data by my business is referred to as "**processing**". As an organisation that decides what personal data is needed to operate or provide my business services, as well as why and how it is processed, I am referred to as the "**controller**". I do not engage the services of any other organisation or company which involve the processing of my customer data (referred to as "**processors**").

My data protection procedures apply a risk based approach, implementing appropriate organisational and technical measures to ensure a level of security appropriate to the risks of personal data being misused. Analysis of such risks, along with descriptions of my mitigatory procedures, can be found in my Business Risk Assessment ("BRA") and my Technology Risk Assessment ("TRA").

Under Article 37 of the Applied GDPR, I, Jonathan Haywood (IOMFSA Designated Business ID #185), act as the Data Protection Officer ("DPO") for my sole trader business.

2. Public Privacy Notice

This notice represents an overview of the full policy.

My data protection principles

While processing personal data I follow six key principles:

1. Personal data shall be processed **lawfully, fairly, and in a transparent manner** in relation to the data subject.
2. Personal data shall be collected for **specified, explicit, and legitimate purposes**, and not further processed in a manner that is incompatible with those purposes.
3. Personal data shall be **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed.
4. Personal data shall be **accurate and kept up to date**.
5. Personal data shall be kept in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which the personal data are processed.
6. Personal data shall be processed in a manner that **ensures appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Why do I collect your personal data?

- Access to your identity data, bank account details, and historic trading activity, allows me to provide a rapid, automated service without the need to perform repeated additional checks.
- By proving your identity, bank account holdership, "liveness" (that you are who you say you are, and that you are present at the time of verification), and your intention to buy cryptoassets, you help to protect me from criminals who may manipulate victims or misuse bank accounts. Stating your source of cryptoasset funds (when selling cryptoassets to me) you protect me from the exchange of illicitly-sourced funds.
- British legislation requires cryptoasset service providers to collect, verify, and store customer data, relating to their identity, their source of funds, their intended business relationship, and whether they have any ties to high risk jurisdictions or to public officials.

What data do I collect and how do I collect it?

- **From your identity document:** Full name, nationality, place of birth, date of birth, and document expiry date.
- **From your bank statement:** Your address, your account number and sort code, and your recent transactional activity.
- **From your video declaration (cryptoasset buyers):** Your "liveness", your intention to buy cryptoassets, your source of funds, and your intended use of the cryptoassets that you are buying from me.
- **From your stated source of cryptoassets (cryptoasset sellers):** Your source of (cryptoasset) funds that you are selling to me.
- **From any external communications (where applicable):** Your telephone number and/or email address.
- **From intermediary trading platforms (e.g. LocalBitcoins, LocalCoinSwap, ZedZeroth.com etc.):** Your platform username, IP geolocation (country only), and the country of your registered phone number (where applicable).
- **From our trade history:** Date/time of transactions, amount of fiat/cryptoassets transacted, and blockchain data (where applicable).

How do I use your data and who do I share it with?

- **Trading procedures:** Your name, identity document expiry date, account numbers and sort codes, contact details, and transactional history, are used during each of our trades to ensure that your payment comes from a verified bank account, that you are trading within your limits, and that your identity documents on file are still valid.
- **Risk assessments:** In order to comply with legislation and to protect my business from exploitation by criminals, all of your data may be used to estimate the degree of "risk" that you present. Customers with an unacceptably high risk score may be declined business.
- **Banking partners, regulators, and law enforcement:** For higher risk transactional activity I may be required to share your data with my banking partner (Enumis Ltd), my regulator (IOMFSA), or law enforcement bodies (such as IOMFIU or UK/IOM police).

Where do I store your data and for how long?

Your submitted identity documents, bank statements, and video declarations, are moved to two devices (each backing up the other) that are:

1. Stored in a secure location.
2. Air-gapped (not connected to the internet)
3. Encrypted with Linux Unified Key Setup (LUKS) Full Disk Encryption (FDE).

The only data stored on active devices is alphanumeric data required during trading procedures (see above). My active devices are also LUKS FDE encrypted and protected by multiple other security measures.

Legislation requires that I store your data throughout the time in which you are actively trading with me, and for a further five years after our final trade (should you cease trading with me).

Can you request access to your data, or its erasure?

I am required to be transparent as to what data I hold for you, with the exception of any information that may be connected to investigations into criminal activities. After our first transaction, legislation prohibits me from deleting any of your data for a five year period. As the Data Protection Officer of my business, you can contact me at zed@zedzeroth.com regarding my use of your personal data.

Can you provide false data?

By providing me with your documents and personal data, you are also confirming that the information is true and accurate. Providing falsified or misleading information could be classed as an offence.

3. Reasons for data collection

My business collects the minimum necessary personal data required to fulfil the following three purposes:

3.1. Business service provision

By collecting data such as a customer's full name, platform usernames, bank account details, and historical transactions, I am able to provide a quick and reliable semi-automated exchange service. Without such data, details would need to be reconfirmed with each trade, considerably slowing the customer experience and leading to a greater chance of errors being made.

3.2. Protection from criminal activity

Verifying customer identity, bank account holdership, source of funds, "liveness", and intention to purchase cryptoassets, protects my business from exploitation by criminals. This includes protection from money launderers and terrorist financers (see "Legal basis for collection"), and also from hackers, con artists, and identity thieves, who can otherwise use compromised bank accounts or manipulated victims in oder to convert stolen fiat funds into unrecoverable cryptoassets.

3.3. Regulatory requirements

See the below section "Legal basis for collection".

4. Legal basis for collection

As a business involved in the exchange of convertible virtual currencies ("CVCs"), specifically cryptoassets, for fiat currencies, specifically British Pound Sterling ("GBP"), with business operations based in the Isle of Man, I am required to register as a "Designated Business" with the Isle of Man Financial Services Authority ("IOMFSA") and to comply with the Isle of Man Government's Anti-Money Laundering and Countering the Financing of Terrorism Code 2019[1] ("The Code"), the Proceeds of Crime Act 2008 ("POCA")[2], the Anti-Terrorism and Crime Act 2003 ("ATCA")[3], and the Proceeds of Crime (Prescribed Disclosures) Order 2015 ("POC (PresDisc) Order 2015")[4].

This legislation requires that, for all customers, I collect the full name, date of birth, place of birth, residential address, source of funds (including the activity that generated the funds, their geographic source, and the customer's account/transaction details for any involved banks, exchange platforms, and blockchains), their intended purpose of business (including the destination of funds), and whether or not the customer is a politically exposed person ("PEP")[5] or if they have ties to sanctioned / higher risk jurisdictions[6]. For customers operating as companies, I am also required to collect their registered company name/number, business address, and details from their certificate of incorporation.

Legislation also requires me to analyse customer data in order to assign risk scores and generate an individual Customer Risk Assessment ("CRA") for each customer.

---

1 https://www.gov.im/media/470621/anti-moneylaunderingandcounteringthefinancingofterrorismcode2019.pdf

2 https://www.iomfsa.im/media/2079/proceedsofcrimeact2008.pdf

3 http://www.legislation.gov.im/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0006/Anti-TerrorismandCrimeAct2003_1.pdf

4 https://www.tynwald.org.im/business/opqp/sittings/Tynwald%2020142016/2015-SD-0327.pdf

5 https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf

6 https://www.gov.im/about-the-government/departments/home-affairs/chief-executives-office/anti-money-laundering-legislation-and-countering-the-financing-of-terrorism-amlcft/

5. Types of personal data

A full explanation of all types of personal data that may be collected by my business is included in Section 5.1 (“Customer due diligence requirements”) of my Anti-Money Laundering & Countering the Financing of Terrorism Policy. I do not collect any “Special Categories” of personal data (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person’s sex life or sexual orientation).

A copy of Section 5.1 of the 16 September 2022 version (Version 5.4) of my Anti-Money Laundering & Countering the Financing of Terrorism Policy is shown here:

Information collection is based on FATF’s [“Financial Action Task Force”] key principles which are summarised as:

“using reliable, independent source documents, data or information; identifying the beneficial owner; understanding and obtaining information on the purpose and intended nature of the business relationship; and conducting ongoing due diligence on the relationship and scrutiny of transactions”[7].

An accumulation of documents from multiple independent sources, each supporting one another (a “cumulative approach”) mitigates the risk of falsification or identity theft. Documents are securely transmitted (E2E encryption) and stored (air-gapped and LUKS FDE) as recommended by FATF. There is no involvement or reliance on third parties, and no “introduced business”, for any element of my CDD processes. A failure/refusal to disclose information must be treated as an ML/FT red flag and taken into account in their CRA. The documentation required in order to verify each customer’s identity, exchange activity (including their intended purpose and source of funds), and locational ties, is outlined below.

Identity

I independently verify every individual customer’s identity with absolutely no reliance on, or outsourcing to, third parties. The Proceeds of Crime Act 2008 (“POCA”), Anti-Terrorism and Crime Act 2003 ("ATCA"), and Proceeds of Crime (Prescribed Disclosures) Order 2015 (“POC (PresDisc) Order 2015”) define “customer information” in the context of “customer information orders” which are submitted when making external disclosures and may be used in money laundering or terrorist investigations. Identity is verified via passports, UK/IOM driving licences, or British Residence Permits. These must be of a high enough resolution and clarity to be fully legible and show all security features, such as holograms, watermarks and machine readable code. Such documents are matched to templates where possible and new documentation is requested whenever those on record expire. Identity and “liveness” is further verified by a clear “selfie” video of the customer reading a unique script (“anti-impersonation measures”). This enables (1) the customer’s face to be matched to their photographic identity document, (2) the identity document itself to be visible in the video in possession of the customer, (3) confirmation that the customer is present at the time of onboarding with a clear intention of trading CVCs via my business.

[7] https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf

Below is a list of identity information that is collected. Note that those items marked with a "*" are always verified with supporting documentation. Other items may be verified based on related risk factors.

- Identity information mentioned by POCA, ATCA, or POC (PresDisc) Order 2015 that I collect and verify for all natural persons and company directors:
    - * Full name: Forename(s) and surname
    - * Date of birth
    - * Place of birth ("POB")
    - * Most recent permanent residential address
    - * Gender: Male, female, or other
- Additional identity information mentioned by POCA, ATCA, or POC (PresDisc) Order 2015 that I collect and verify for companies. I only form business relationships with companies incorporated in the UK or the Isle of Man, and I verify their details, including officer identities, via the official government registries [8] [9]:
    - * Registered company name and number
    - * Business address
    - * Certificate of incorporation including country and date of establishment
- Other identity information that I always collect:
    - Nationality (verified on passports & BRPs, but not driving licences)
    - * An official personal identification number such as passport number ("PN"), driving licence number, or BRP number
    - * Identity document expiry date
    - Details of any public or high profile positions held
    - IP address, timestamps, geo-location data, and device identifiers
- Other information that I may collect depending on circumstances:
    - Telephone number
    - Email address
    - Exchange platform username(s)
    - Occupation
    - Name of employer
    - A description of any business which the person/company carries on
- Identity information mentioned by POCA, ATCA, or POC (PresDisc) Order 2015 that I deem unreasonable to collect and/or verify:
    - Title (e.g. Mr, Mrs etc.)
    - Previous residential/business addresses

[8] https://find-and-update.company-information.service.gov.uk/
[9] https://services.gov.im/ded/services/companiesregistry/companysearch.iom

Intended purpose of business relationship / nature of activity

The customer's purpose / intended nature of relationship must be established. This includes the "beneficiary information" or the destination of the exchanged funds. There must be ongoing and effective monitoring of the customer's exchange activity. This includes:

- Ongoing recalculation of risk scores based on trade-by-trade volume/velocity figures.
- Continual checks that customer exchange activity matches their stated intentions.

Source of funds and/or wealth

The customer's source of funds ("SOF") must be established (sometimes referred to as "originator information"). Bank account holdership and transactional history is verified via original PDF statements downloaded directly and recently from the customer's banking application. Up-to-date SOF documentation is requested when necessary. This includes:

- The activity that generated the funds that are to be exchanged.
- The means by which the funds have been transferred from their source.
- Unique identifiers such as: bank account details, exchange platform usernames and trade identifiers, CVC addresses and blockchain transaction identifiers, and IP addresses.
- Geographic source.
- Any significant linked funds that the customer has received from a third party, that are not clearly from wages, business, or investments, may require further verification of the true source, including verification of the third party's identity and their relationship to the customer.

Higher risk customers

- Additional identity verification and further research should be considered.
- Verification of SOF should be considered. The stated source can be corroborated with reliable, independent source documents establishing the activity that generated the funds, and the means of transfer. Funds moved from another source (e.g. another bank account whether in the customer's name or the name of a third party) may require documentation establishing and verifying the original source.
- Ongoing and effective *enhanced* monitoring of the customer's activity should be considered.

Higher risk domestic PEPs and all foreign PEPs (of any risk classification)

- There *must* be ongoing and effective enhanced monitoring of the customer's activity.

Customers of high net worth

- The customer's source of wealth may need to be established. This should give a broad understanding of their entire body of wealth and total assets, including wealth in the form of family/inherited wealth, income/business wealth, and investment wealth.

6. Collection methods

6.1. Direct collection

When onboarding new customers ("verification"), all customers send me:

1. A clear photo of their passport's photo page or both sides of a UK driving licence / British Residence Permit.
2. A PDF statement downloaded directly from the banking app/website for each bank account that they would like to use to make payments. These must be original PDF files, not screenshots, and must include:
    a. The last two months of activity
    b. Their full name
    c. Their sort code and account number
    d. Their address

Customers purchasing cryptoassets send an additional video of themselves holding their identity document next to their face while reading the following five sentences:

1. "I, [THEIR FULL NAME], am buying cryptocurrency from Jonathan Haywood for my own use and not under pressure from anyone else."
2. "I understand that if I send cryptocurrency to someone else then I may never get it back."
3. "[THEIR PLATFORM USERNAME / EMAIL ADDRESS] is my own account and under my control."
4. "The money I am using to buy cryptocurrency comes from [THEIR SOURCE OF FUNDS e.g. salary, savings…]."
5. "I am buying cryptocurrency to use for [THEIR INTENDED USE e.g. investing, purchasing goods online, international transfers…]."

Customers selling cryptoassets send an additional sentence explaining how they bought the funds that they are selling and why they are selling it (the "fiat onramp").

In addition to the above submitted files, I may ask for the customer's telephone number or email address for communication purposes. Email addresses are also used for placing orders on ZedZeroth.com.

6.2. Indirect collection

Data is also collected directly from intermediary trading platforms. This includes the customer's platform username, IP geolocation country, and the country of their registered phone number (where applicable).

Details from each customer transaction ("trade") is also stored, such as the date/time of transcation, the amount of crypto/fiat exchanged, and blockchain data where applicable.

7. Use of personal data

As explained in the “Reasons for data collection” section, a customer’s personal data is used in a number of ways. Name, identity document expiry date, bank account numbers and sort codes, contact details, and transactional history, are used during each transaction to provide an efficient semi-automated service. Such data also ensures that payments come from the correct bank account, that customers are trading within their limits, and that their identity document on file is still valid (not expired).

Aspects of each customer’s personal data is also converted into a series of risk scores, which are combined to calculate an overall customer risk score, used as part of my required Customer Risk Assessments (“CRAs”). These assessments are then used to determine “higher risk” customers who may be required to undergo “enhanced customer due diligence” (“ECDD”) measures. Customer’s for whom risks cannot be mitigated to within acceptable tolerances (my “risk appetite”) may face trading restrictions or may be declined business.

8. Sharing of personal data

My banking partner, Enumis Ltd, monitors all of my business banking transactions and is required to comply with UK financial regulations under the supervision of the UK Financial Conduct Authority (“FCA”). For transactional activity that they determine to represent a higher risk, they may request relevant customer data as part of their own compliance procedures.

My business is also subjected to occasional inspections by my regulator, the Isle of Man Financial Services Authority (“IOMFSA”). They may request to check the personal data of individual customers, or I may be required to grant them access to all my business records, including all customer data and files. Such inspections may be related to investigations into specific customers, but also serve as confirmation that I am complying to the legal requirements described in the “Legal basis for collection” section.

As the Money Laundering Reporting Officer (“MLRO”) of my business, I am required to submit a Suspicious Activity Report (“SAR”) to the Isle of Man’s Financial Intelligence Unit (“IOMFIU”) “in respect of information that comes to me in the course of my business, if I know or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in (or attempting) money laundering or terrorist financing”. These SARs may include a customer’s personal data.

If I have reasonable grounds for knowing or suspecting that any customers (or their funds) are connected to criminal activity, I may be required to send customer data to law enforcement bodies such as IOMFSA or relevant police forces. I am also required to grant local law enforcement access to any relevant data that they should request.

9. Storage and security

9.1. Data storage

Customer documentation such as copies of identity documents, bank statements, video declarations, and source of funds screenshots, are permanently removed from my active business devices every week, and transferred to two dedicated secure storage devices. These storage devices are stored in a secure location, air-gapped (no active network connection), and encrypted with Linux Unified Key Setup ("LUKS") Full Disk Encryption ("FDE").

Processed data such as customers' names, identity details, bank account details, and exchange activity, that are stored on active business devices are also secured with LUKS FDE among other security measures.

9.2. Data breaches

I implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk that my data processing poses to my customers. This includes the risk caused by accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, each customer's personal data.

In the event of a data breach I will:

- Take steps to investigate the breach.
- Record the incident, including the facts, the effects, and any remedial action taken.
- Inform the Isle of Man Information Commissioner within 72 hours of becoming aware of the breach, unless the data breach is unlikely to result in any risk to the rights and freedoms of my customers.
- Inform any customers if it is likely that the breach will result in a high risk to their rights and freedoms.

10. Storage time scales

As specified in the Isle of Man Government's Anti-Money Laundering and Countering the Financing of Terrorism Code (2019)[10], I am required to store customer data for at least five years following the end of our business relationship (our most recent / final transaction).

---

10 https://www.gov.im/media/470621/anti-moneylaunderingandcounteringthefinancingofterrorismcode2019.pdf

11. Customer rights and data access

This policy acts as a transparent description of my customers' personal data that I collect, control and process. As the Data Protection Officer ("DPO") of my business, customers may contact me at jhaywood@protonmail.com in order to obtain a copy of all the data that I hold for them. Information connected to criminal investigations may not be provided under "tipping off" legislation.

After initiating a business relationship (engaging in our first exchange transaction or "trade") customers cannot request that I erase their data as I am required to hold it for a minimum period of five years after our final transaction.

12. Offences for providing false or misleading information

Customers who deliberately or negligently provide false or misleading information for their own gain may be committing fraud. I am required to report suspicious behaviour regarding information provision to IOMFIU, this includes reluctance to provide required or relevant information relating to identity, source of funds, or geographic/political ties.

13. Documentation

In writing this policy I referred to the following documentation:

Basic compliance guide
https://www.inforights.im/media/1785/2020-basic-compliance-guide.pdf

Compliance guide for smaller businesses, charities and other organisations
https://www.inforights.im/media/1586/introduction-to-the-new-isle-of-man-data-protection-law.pdf

Compliance self-help checklist
https://www.inforights.im/media/1810/controller_checklist.pdf

Requirements infographic
https://www.inforights.im/media/1588/basics_infographic.pdf

A closer look at “Principles”
https://www.inforights.im/media/1895/principles_reviewed-january-2021.pdf

A closer look at “Transparency”
https://www.inforights.im/media/1442/transparency.pdf

GDPR Toolkit Part 1, V 2.0, March 2021
https://www.inforights.im/media/1916/compliance_part-1_5-ws_data-mapping_reviewed-march-2021.pdf

GDPR Toolkit Part 2, V 2.0, March 2021
https://www.inforights.im/media/1917/compliance_part-2_-accountability_reviewed-march-2021.pdf