UKPOSTBOX

Data Handling & GDPR

Learn about the processes we have in place and how your data is handled.

Table of contents

Committed to responsible & secure data protection

UK Postbox is committed to securely handling, storing and disposing of all customer data, as well as being clear on how we achieve this, and what happens to your data throughout the entire process. We have distinct policies for both the physical and digital handling of mail that detail the actions we're taking, as well as our GDPR statement.

Because we know that our personal and business customers use our service in varying ways, we've created the below flow to illustrate what's happening to your data and mail items throughout the lifecycle of UK Postbox.

1. Creating your account

When signing up to our service, we're required by law to collect sufficient evidence to confirm your identity. This process, named Know Your Customer (KYC), requires you to upload some of your personal documents and data such as a passport, driving license or identity card.

We request this information solely for the purpose of confirming your identity, and we will securely store the records needed for us to comply with legal requirements in our cloud storage solution.

All customer information is processed and handled in compliance with the General Data Protection Regulatory (GDPR), and we only request information that is necessary to create your account.

2. Our secure mailing facility

Once you've signed up, the first touchpoint with your physical mail items is when something arrives for you at your UK Postbox address. All mail is delivered to our secure mail sorting facility, which is protected by CCTV, locks and alarm systems, reinforced fencing and gated access. A security cleared team member must accompany all site visitors, and public access to the site is not permitted. A trained member of staff will receive all mail delivered by pre-approved couriers before being deposited in our mailroom, ready for processing.

3. Physical & digital processing of your mail

Members of our mail processing team will then upload a scan of the outside contents of mail items before assigning a unique barcode and sending a notification to your account. Alternatively, if you've set up an automatic workflow and request mail is open and scanned upon receival, the mail contents will be viewable from your account.

Once your mail has been digitised, the scanned image is stored in the Azure UK South data center, a secure cloud platform provided by Microsoft. Using our online mail management platform, iPostalMail, individuals can request certain actions for their mail items which will be carried out by a member of the team. Until you let us know what to do next, we'll store your physical mail items within our secure facility.

4. Online mail management

Our online mail management platform has been developed using secure coding techniques, and your account is protected through a variety of security practices we have implemented. Access to your account is limited by authentication and session expiry, and individuals have the option to add Two-Factor authentication for an additional level of protection. Using this platform, you can request different actions for your mail items such as forwarding, storing or destroying.

What happens to your data next depends on the actions you take from your account, and we've provided examples below to demonstrate how your data is affected:

Scanning

The envelope is opened and the contents are scanned into a PDF document, which is sent to your account and stored in the cloud. Our team will only open mail when requested, and treat each item with the utmost confidentiality. We'll return the physical item to safe storage after uploading your scan.

Forwarding

The envelope is opened and the contents are scanned into a PDF document, which is sent to your account and stored on the cloud. Our team will only open mail when requested, and treat each item with the utmost confidentiality. We'll return the physical item to safe storage after uploading your scan.

Digital Store

Once you have scanned the pages of a letter, you can store it digitally in our platform. This means that you then have the option for the physical item to be destroyed, leaving only the digital version accessible through your account with us. All files are stored in our secure cloud provider Microsoft Azure.

Physical Store

If you don't want to forward or destroy your original offline mail items, you can physically store them at our secure facility for later action. Storing physical items is a chargeable service depending on your plan, and we have several physical security measures in place to restrict access.

Recycled

We shred elements of your items that are deemed confidential but process the remaining contents and packaging for recycling. We do not hold any record of the physical item following this action.

Shredded

Request that we destroy your physical mail item in a secure way. All mail items are shredded on-site by Restore Datashred, and we will keep no physical copy of the item.

Message Centre

If you contact us within our platform, you'll enter an instant messaging conversation with a member of our team. All chats are logged for reference at a later date, but will only be used in relation to resolving a problem with your account.

Send Letters

Upload a document or PDF that you'd like us to send on your behalf, and we'll handle the printing, packaging and posting of the mail item. This request will be treated with utmost confidentiality by a trained member of staff, and a digital copy of the item will be stored securely.

Integrations

Integrating your account with popular workflow and cloud storage solutions such as Google Drive and Microsoft OneDrive means that you approve the transfer of data from our servers to your internal data providers. We will hold a digital copy of the item unless you request that it is destroyed, however we have no control of the data once it has been passed to your internal storage solutions.

Fulfilment

When fulfilling orders on your behalf, a trained member of the dropshipping & fulfilment team will have to view and process customer information in order to fulfil the order. We do not retain or store your customer data on our servers, and only access this information when a fulfilment has been requested from your account.

If you have any questions, would like to make a request, or need to contact us in relation to data handling and GDPR, contact our Data Protection Officer (DPO) by emailing: managers@ukpostbox.com.

GDPR Statement

As part of our commitment to data handling and the GDPR, we regularly review and update our internal practices, processes and documentation regarding how we handle your data, the rights an individual has, and the actions taken in the event of a data breach.

Commitment

UK Postbox is committed to the practices outlined in the GDPR, and follows the guidance around privacy by design, the right to be forgotten, consent, and a risk-based approach. Our aims are to:

1. Offer complete transparency regarding how we handle and use data.
2. Only process data in a lawful, fair and transparent way for necessary purposes.
3. Ensure all data is up to date, accurate and removed when redundant.
4. Safely and securely handle and process any data.

Staffing

We have assigned a designated Data Protection Officer (DPO) who has received training and holds responsibility for promoting awareness of GDPR throughout UK Postbox. Their role is to demonstrate best practice and support employees throughout the workforce to ensure data is being handled compliantly.

Policy

We have a dedicated privacy policy which is available online and sent to all employees, contractors and suppliers associated with our services. As part of our induction training for new staff, employees are required to digest our policies and attend follow-up sessions following a change in legislation.

Right to be forgotten

We recognise and practice the right to be forgotten, also known as the right to erasure. As outlined in Article 17 of the GDPR, customers have the right to request that their personal data is erased without delay.

Subject access requests

Individuals have the right to submit a request for their personal data and other related information to be provided within one month of the initial submission. In most cases, there will be no charge for this request, unless it is unfounded, excessive or repetitive. In these cases, we may charge a 'reasonable fee' due to the works involved. Individuals can contest this decision with the supervisory authority (the Information Commissioner's Office (ICO) if they deem a charge to be unfair.

Privacy

We will implement data protection "by design and by default", as required by the GDPR. Safeguards will be built into products and services from the earliest stage of development and privacy-friendly default settings will be the norm. The privacy notice, which is on our website and which is provided to anyone from whom we collect data, explains our lawful basis for processing the data and gives the data retention periods. It makes clear that individuals have a right to complain to the ICO. We have conducted a privacy impact assessment (PIA) to ensure that privacy risks have been properly considered and addressed.

Privacy Information Notice

Our privacy notice has been made readily available and details who we collect data from, how we process data, and the data retention period. The privacy information notice for website visitors can be accessed here: https://www.ukpostbox.com/legals/privacy-policy.

Data loss

In the event of a data breach that poses a risk to the rights and freedoms of individuals, we will notify these individuals as well as the ICO as soon as possible, within 72 hours of a breach occurring.

Digital Security Statement

UK Postbox takes responsibility to protect and secure your information seriously and strive for complete transparency around our security practices detailed below. Our Privacy Policy also further details the way we handle your data.

Access Control | Admin-side

Access to UK Postbox's technology resources is only permitted through secure connectivity, by authentication, session expiry and IP restricted access. Our production password policy requires complexity, expiration, and lockout and disallows reuse. UK Postbox grants access on a need to know basis of least privilege rules, reviews permissions quarterly, and revokes access immediately after employee termination.

Access Control | Client-side

Access is restricted by authentication and session expiry. Passwords are hashed and salted. All access to client PDFs, thumbnails and data are conducted through the website which is authenticated by user session. Sessions are audited, and users have the option to enable Two-Factor Authentication for an additional layer of security.

Technologies

The core infrastructure is hosted in the Azure Cloud, West Europe and UK South datacenters. The source code for Software developed in house is stored in private repositories on github.com. Access to source code is restricted to users authenticated by senior management.

Development

Our development team employs secure coding techniques and best practices. Developers are formally trained in secure web application development practices upon hire and annually.

Development, testing, and production environments are separated. All changes are peer reviewed and logged for performance, audit, and forensic purposes prior to deployment into the production environment.

Logging

Application and infrastructure systems log information to a centrally managed log repository for troubleshooting, security reviews, and analysis by authorised UK Postbox employees. Logs are preserved in accordance with regulatory requirements. We will provide customers with reasonable assistance and access to logs in the event of a security incident impacting their account.

Encryption / SSL

All communications for websites, services and statistics panels are served over SSL. The SSL certificates are cycled every 30 days.

Email communications

Email communications are not encrypted, and therefore it is the policy of UK Postbox not to use email for sharing confidential information. Any incoming attachments will be removed to ensure that confidential/sensitive attachments are not received. UK Postbox offers secure upload processes to protect customer documentation.

Client Payment / Compliance PCI

UK Postbox is compliant with the Payment Card Industry's Data Security Standards (PCI DSS 3.2) and can therefore accept or process credit card information securely in accordance with these standards. UK Postbox re-certifies this compliance annually. Identifiable payment information is not stored in-house. Stripe.com and PayPal handle card information and provide a token which is used to access funds. No card information other than the last 4 digits are stored in the database or in logging.

Monitoring

UK Postbox maintains a documented vulnerability management program which includes periodic scans, identification, and remediation of security vulnerabilities on servers, workstations, network equipment, and applications. All networks, including test and production environments, are regularly scanned.

Physical Security Statement

In addition to our digital practices, we implement a variety of physical security measures to ensure that your physical data is protected from the moment it's received until you request that it is forwarded or destroyed.

Location Based Security

The offices and warehouses used are protected by a number of physical and digital means. Each premise is protected by a combination of keypads, locks and alarm systems. Only specific keyholders have keys and know the alarm codes. Areas which are more vulnerable to forced entry are protected by reinforced bars or drop doors.

Visitors

All visitors to any premises are accompanied at all times. No one is able or permitted to walk into any warehouse or premises unattended and will be stopped and escorted at all times to an appropriate manager. Client collections are not offered for security reasons.

CCTV

Premises are covered by CCTV, internally and externally. The CCTV can be viewed on and offsite. Recordings are retained for 30 days for security purposes only.

WIFI Security

All WIFI networks are password protected, no networks are open. The credentials for the routers are changed and are stored in a password vault. Visitors are not permitted access to WIFI.

Disposing of Retired Hardware

Computer hardware often contains memory modules that cannot be disposed of in their original state. The IT team ensures that all retired hardware is disposed of in an environmentally responsible manner and pays particular attention to devices that contain memory. Hard drives are destroyed to ensure that client data is not exposed.

Equipment

Staff are not permitted to take or remove any electrical equipment offsite.

Computers

This covers but is not limited to; PCs, Macs, tablets, laptops and statistical displays.

All devices are password protected, have software updates and patches installed when available. Devices have antivirus installed and are scanned daily.

Mobile Phone Use

Staff are not permitted to use mobile phones during work hours. Any individual suspected of or caught taking photographs on premise without management sign off will face disciplinary action.

Shredding

All paperwork containing personally identifiable information and mail items that a client has requested to be shredded, are securely shredded on-site by Restore Datashred.