Privacy Policy

Published by: Stephen Ingram - Data Protection Officer

Date: 08th June 2023

Company: IG Technology Ltd

Last updated date: **[08/06/2023]** IG Technology Ltd.

SCOPE OF POLICY

IG Technology Ltd (**We**, **Us**, **Our**) is committed to protecting and respecting your privacy.

This policy explains how we collect, use, disclose, and safeguard your information when you visit our mobile application. Please read this **Privacy Policy** carefully. IF YOU DO NOT AGREE WITH THE TERMS OF TIS POLICY, PLEASE DO NOT ACCESS THE APPLICATION.

This policy sets out the basis on which any personal data We collect from you, or that you provide to Us, will be processed by Us. Please read the following carefully to understand how We your will treat your personal data.

CHANGES TO PRIVACY POLICY

We reserve the right to make changes to this Privacy Policy at any time and for any reason. We will alert you about any changes by updating the **"Last updated"** date of this Privacy Policy. You are encouraged to periodically review this Privacy Policy to stay informed of updates. You will be deemed to have accepted the changes in any revised Privacy Policy by your continued use of the Application after the date such revised Privacy Policy is posted.

- The Legacy® IPC Mobile Applications hosted on (The App store) is referred to as (**App**), once you have downloaded or streamed a copy of the App onto your mobile telephone, tablet or handheld device (**Device**).

If you have any questions about any of the information or definitions in this Privacy Notice, email us at customer@ig-technology.co.uk.

GDPR- APP COMPLIANCE

At IG Technology Ltd, we take pride in being GDPR compliant. All your data is handled in strict compliance with EU data protection laws.

DATA COLLECTION

By downloading and using this App/Website, you explicitly give your consent to the collection, processing, and use of your personal data in accordance with the App's privacy policy. We may collect data from you in a variety of ways. The information we may collect via the Application depends on the content and materials you use. We will only collect the minimum amount of data to provide our services. **Automatic Data** is not collected (No information is gathered through website visits OR without accessing the App). Data collection will **only** be used upon registration of the App, No data will be shared or used for marketing purposes.

THE LAWFUL BASIS WE PROCESS PERSONAL DATA

The legal basis for which data is collected can vary depending on the specific jurisdiction and the purpose of data processing. However, the following contains an overview of some common legal bases for data collection:

1. **Consent**: Data collection may be based on the explicit and informed consent of the data subject. Consent should be freely given, specific, and revocable at any time. The data controller must provide clear information about the purposes of data processing and any relevant third parties involved.

2. **Contractual necessity**: Data collection may be necessary for the performance of a contract between the data subject and the data controller. For example, when collecting personal data to fulfil an order or provide a requested service, the legal basis may be the necessity to fulfil contractual obligations.

3. **Legal obligation**: Data collection may be necessary to comply with a legal obligation imposed on the data controller. This could include obligations related to tax reporting, regulatory requirements, or law enforcement purposes.

4. **Legitimate interests**: Data collection may be justified by the legitimate interests pursued by the data controller or a third party, provided that these interests do not override the fundamental rights and freedoms of the data subject. Legitimate interests can include purposes such as fraud prevention, network security, direct marketing, or internal administrative purposes.

5. **Vital interests**: Data collection may be necessary to protect the vital interests of the data subject or another individual, particularly in emergency situations where someone's life or physical integrity is at risk.

PERSONAL DATA WE COLLECT

Personal identifiable information submitted may include your name, address, e-mail address, phone number, username and password.

HOW WE USE YOUR PERSONAL DATA

We use your personal data for:

- Creating your online account/registration.
- Managing your online account and activities.
- Customer service- Responding to enquiries.
- Security and Integrity, including fraud prevention, public safety, or enforcement of our policies and procedures.

YOUR RIGHTS TO YOUR PERSONAL DATA

- You have the right to request that we restrict or suppress the personal data that we hold about you.

PROCESSING OF PERSONAL DATA (Data Subject Rights)

You have a number of "Data Subject Rights", we have explained below what they are and how you can exercise them. You can read more about these rights on the Information Commissioner's Office website: https://ico.org.uk.

- **Right of access –** You have the right to request a copy of the personal information that we hold about you.
- **Right to rectification –** If you think that any of your personal information we hold is inaccurate, you have the right to request that it is updated. We may ask you for evidence to show it is inaccurate.
- **Right to erasure –** (also known as the Right to be Forgotten) - You have the right to request that we delete your personal information that we hold.
- **Right to restriction of processing –** You have the right to request we restrict or suppress the personal data we hold about you.
- **Right to data portability –** You have the right to ask us to electronically transfer your personal information to another organisation in certain circumstances.
- **Right to withdraw Consent –** Where we are relying on your consent for processing you can withdraw or change your consent at any time.

PORTABILITY OF PERSONAL DATA

- **Right to data portability –** You have the right to request and receive a copy your personal data in a commonly used and machine-readable format, and in some cases, to have it transmitted directly from one data controller to another, if technically feasible.

RIGHT TO WITHDRAW

- **Right to erasure –** (also known as the Right to be Forgotten) - You have the right to request that we delete your personal information that we hold.

The above rights may be limited in some circumstances, for example, if fulfilling your request would reveal personal information about another person, if you ask us to delete information which we are required to have by law, or if we have compelling legitimate interests to keep it. We will let you know if that is the case and will then only use your information for these purposes. You may also be unable to continue using our services if you want us to stop processing your personal information.

RIGHTS TO AUTOMATED DECISION MAKING, INCLUDING PROFILING

To exercise your right to automated decision-making, you have the following rights:

1. **Right to information**: have the right to be informed when their personal data is subject to automated decision-making, including profiling. They should be provided with clear and transparent information about the logic, significance, and consequences of such processing.

2. **Right to human intervention**: Users have the right to request human intervention in the decision-making process. This means that they can ask for a decision to be reviewed or reconsidered by a human being, or they can provide their own input or explanation in the decision-making process.

3. **Right to challenge and obtain explanations**: Users have the right to challenge the automated decision and obtain an explanation for the decision reached. They should be able to understand the logic behind the decision and how their personal data was used in the process.

4. **Right to object**: Users have the right to object to automated decision-making, including profiling, if they believe it has a negative impact on their rights, freedoms, or legitimate interests. In such cases, the organization must reconsider the decision or provide compelling legitimate grounds to continue the processing.

It's important to note that there are certain exceptions to the right to automated decision-making, such as when the decision is necessary for the performance of a contract, authorised by law, or based on explicit consent. The specific rights and requirements may vary depending on the applicable data protection regulations in a particular jurisdiction.

If you have any general questions or want to exercise any of your rights, please contact customer@ig-technology.co.uk.

We encourage you to get in touch if you have any concerns with how we collect or use your personal information. You have the right to lodge a complaint directly with the Information Commissioner's Office, the data protection regulator in the UK, you can do this by visiting the ICO website: https://ico.org.uk/make-a-complaint/.

GLOBAL PRIVACY NOTICE

IG Technology Ltd is committed to handling your personal information or personal data ("Personal Data") responsibly and transparently. This Global Privacy Notice ("Notice") is intended to comply with the relevant transparency requirements under the applicable privacy or data protection laws.

CHILDREN'S POLICY

The Legacy® device is available to adults aged 21+ on prescription only. IG Technology Ltd does not envision that users under this age will access the Legacy® App. If We learn of any data collected by this group, it will be deleted.

DATA BREACH

Data is gathered when you request a Data Breech form on our website, and/ or report a problem with Our App/Site. The information you give Us may include your name, address, e-mail address, username, password, personal description, and any other information you provide.

HOW IS YOUR DATA STORED

All information you provide to Us is stored on secure servers held in both the European Economic Area (**EEA**) and GDPR compliant international data processors only. Where international data processors are used, all appropriate technical and legal safeguards will be put in place to ensure that you are afforded the same level of protection as within the EEA.

THIRD PARTY ONLINE/MOBILE STORES

User's personal data **will not** be shared with any other parties.

This Privacy policy does not apply if users follow links to third party websites. Users should make themselves aware of third party policies.

This Privacy policy does not apply to the third-party online/mobile store where you install the Application, including any in-app virtual items, which may also collect and use data about you. We are not responsible for any of the data collected by any third hand party.

COOKIES AND TRACKING TECHNOLOGY

Under Data protection (GDPR), cookie IDs is considered personal data. A cookie ID is the identifier that is included within most cookies when set on a user's browser. It is a unique ID that allows your website to remember the individual user and their preferences and settings, when they return to your website. You can click to opt out of having the Platform used to select ads for your browser based on your online web browsing behaviour.

YOUR RIGHTS REGARDING YOUR PERSONAL DATA

Under applicable data protection laws, you have the right of access, the right to rectification or the right to erasure of your data.

Please contact us if you wish to make a request, customer@ig-technology.co.uk.

Under General Data Protection Regulation (GDPR), IG Technology Ltd is required to respond to any requests without undue delay and within one month of receiving the request. This time frame could be extended by an additional two months in certain complex cases, but the user would be informed about the extension and the reasons for it within one month of receiving the initial request.

Please note however, that this time frame is a general guideline and not an absolute rule. Different jurisdictions may have different requirements, and specific circumstances of the request can also impact the response time. For instance, if the request is complex, involves a large amount of data, or requires additional verification, it may take longer to provide a response.

RETENTION OF PERSONAL DATA

Under GPDR, 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. We hold your personal information for as long as we have a legal or business reason to do so, which generally means as long as you remain a User of the Legacy® IPC system or as required to meet our legal

obligations, resolve disputes or enforce our agreements. To fulfil our obligations to the NHS, regulatory or similar bodies, health-related personal information may need to be retained for a period of time after you cease to be a User of the Legacy® IPC system. We'll always store your data securely and won't use it for any other purpose.

SITE SECURITY

IG Technology Ltd is committed to securing the safety of our site and personal data.

- Enforce secure communication. Safeguard communication on the App.
- Provide the right permissions. Use intents to defer permissions.
- Store data safely. Store private data within internal storage systems.
- Keep services and dependencies up to date.

For a comprehensive guide to Site security, please refer to our Cybersecurity policy (www.ig-technology.co.uk).

DESTRUCTION OF DATA

This policy establishes guidelines and procedures for the secure and proper destruction of sensitive data to mitigate the risk of unauthorized access or data breaches. It is the responsibility of all employees and authorised individuals to adhere to this policy when disposing of data-bearing assets.

1. Definitions: a. Sensitive Data: Any information that, if accessed by unauthorised individuals, could cause harm to individuals, the organisation, or violate applicable laws and regulations. b. Data-Bearing Assets: Any physical or electronic media, including but not limited to hard drives, solid-state drives, USB drives, CDs/DVDs, tapes, or any other storage devices containing sensitive data.
2. Classification of Data: a. The organisation shall classify data based on its sensitivity and define data retention periods. This classification will determine the appropriate destruction methods.
3. Destruction Methods: a. Physical Destruction: Data-bearing assets that are no longer required shall be physically destroyed using approved methods, such as shredding, crushing, or incineration, to render the data irrecoverable. b. Secure Wiping: For electronic storage media, approved secure wiping methods, such as data erasure software using industry-recognised standards, shall be employed to ensure complete and irreversible removal of data. c. Degaussing: Magnetic storage media, such as tapes or hard drives, shall undergo degaussing using approved equipment to erase all data.
4. Data Destruction Procedures: a. Employees or authorised individuals responsible for data destruction shall follow documented procedures that outline the steps to be taken for each destruction method. b. The destruction process shall be logged, including details such as the date, type of media, destruction method used, and the individual performing the destruction. c. Destruction procedures shall include verification steps to ensure successful data destruction and proper disposal of the destroyed media.
5. Disposal of Destroyed Media: a. Disposal of destroyed media shall be carried out in a secure manner to prevent any possibility of data recovery. b. The organisation shall maintain relationships with authorised recycling or disposal vendors to ensure compliance with environmental regulations and secure disposal practices.

6. Employee Training and Awareness: a. Regular training and awareness programs shall be conducted to educate employees and authorised individuals on the data destruction policy, procedures, and the importance of proper data disposal. b. Employees shall be made aware of the consequences of non-compliance with this policy, including disciplinary actions and potential legal repercussions.
7. Audit and Compliance: a. Regular audits shall be conducted to ensure compliance with the data destruction policy. b. Compliance with this policy shall be monitored, and any deviations or non-compliance shall be addressed promptly.
8. Policy Review: a. This policy shall be reviewed periodically to ensure its relevance and effectiveness in addressing emerging threats and changes in data protection regulations. b. Any necessary updates or revisions to this policy shall be communicated to all employees and authorised individuals.
9. Policy Violations: a. Violations of this policy shall be reported to the appropriate authority for investigation and may result in disciplinary action, up to and including termination of employment or legal consequences.
10. Policy Distribution: a. This policy shall be communicated to all employees and authorised individuals and made readily accessible through appropriate channels, such as the organisation's intranet or employee handbook.

MANAGING DATA CONFIDENTIALITY- BREACHES

We prioritise the protection of your personal information and understand the importance of maintaining its confidentiality. In the event of a data breach, we have implemented a comprehensive approach to manage and address such incidents:

1. **Rapid Response**: We have established an incident response team that is promptly activated upon discovery of a data breach. This team comprises experienced professionals who are trained to assess and mitigate the impact of the breach.

2. **Investigation and Containment**: Our team conducts a thorough investigation to determine the extent and nature of the breach. Immediate measures are taken to contain and minimize any further unauthorized access to your data.

3. **Notification**: If we determine that the breach poses a significant risk of harm to your privacy or rights, we will notify you without undue delay. Our notification will provide clear and concise information about the breach, the types of data affected, and the steps you can take to protect yourself.

4. **Assistance and Support**: We are committed to assisting you throughout the process. Our team will offer guidance and support to help you mitigate any potential adverse consequences resulting from the breach.

5. **Remedial Actions**: Following a data breach, we take proactive steps to address vulnerabilities and enhance our security measures. We assess our systems, policies, and procedures to identify areas for improvement and implement appropriate measures to prevent future incidents.

6. **Compliance and Transparency**: We comply with applicable laws and regulations regarding data breach notifications. We work transparently with regulatory authorities and cooperate fully during investigations.

7. **Continuous Monitoring**: We maintain on-going monitoring and surveillance of our systems to detect and respond to any suspicious activities or potential breaches. This proactive approach enables us to take immediate action, further safeguarding your personal information.

Our commitment to your privacy and data security remains unwavering. In the unfortunate event of a data breach, we will act swiftly and responsibly to protect your information, keep you informed, and strengthen our measures to prevent similar incidents in the future. For more information - see our Cybersecurity policy (www.ig-technology.co.u).

For the purpose of the Data Protection Legislation, the Controller is IG Technology Ltd:

IG Technology Ltd
Wylcut House
316 Petre Street
Sheffield
S4 8LU
United Kingdom

The Data Protection Officer for the Legacy® IPC App is Stephen Ingram.

Email: Stephen.ingram@ig-technology.co.uk