

## PRIVACY POLICY

# Our Commitment to Protecting Your Privacy

### VERSION 3: EFFECTIVE AS OF 1 DECEMBER 2024

This Privacy Policy explains how the Shift4 group, consisting of – Shift4 Limited, Shift4 Payments UK Limited, Shift4 Technology Limited, Shift4 Solutions Limited or any other relevant Shift4 group affiliate (“collectively “Shift4” “our” “us” or “we”) – uses your personal data. Please read this Privacy Policy carefully.

We provide B2B payment processing services, including acquiring services, banking products and related services, and other ancillary products and services (“Shift4 Services”). We are committed to respecting your privacy and protecting your personal data in accordance with the General Data Protection Regulation and the UK’s Data Protection Act 2018 (together, “Data Protection Regulations”).

By accessing, browsing, or using our websites, or during the process of becoming one of our clients, or as an employee or candidate, you are confirming that you have read, understood, and agree to the terms of this Privacy Policy. We regularly review this Privacy Policy and may make updates from time to time. To the extent that we make a material change we will post a notice on our website. You are advised to visit this page regularly to check for updates.

#### **WHAT, WHEN, AND WHY WE COLLECT YOUR DATA**

We collect and use your personal data as a Controller in the following instances: when you, an individual, are (i) accessing, browsing, or using our websites; (ii) in the process of becoming one of our clients; (iii) a person that has filled out an application form; (iv) an employee or candidate. Personal data means any information about you that can identify or help identify you.

#### **We collect the following personal data when you access, browse, or use our website:**

Technical data including IP address, login data, details about your browser, length of visit to pages on our website, page views and navigation paths, details about the number of times you use our website, time zone settings and other technology on the devices you use to access our website; cookies; personal data that you post to our website or other social media including if you are asked to enter personal detail online to receive more information about our services.

For more information about our cookie policy please click [here](#).

We use your personal data to track site usage, to assist in product development, monitor behavior for marketing purposes, and to connect with you if you have provided your personal data to receive more

information. We use this data to serve ads through ad platforms on other sites and also use it to operate our website and ensure relevant content is provided to you; to ensure the security of our website; to maintain back- ups of our website and/or databases; and to enable publication and administration of our website, other online services, and business.

We collect the following personal data when you are a client or are in the process of becoming a client:

Personal data that you provide us if you want to become, or you are, a client, such as your name, identification number, date of birth, email address, phone number, location/address, additional personal identification documents, and any other personal data and any documents necessary to carry out customer due diligence and “kyc” requirements including personal data found in your application form or agreement for services; Information provided at trade shows or events; Additional information provided during the course of engagement for legitimate reasons.

We use your personal data to collect and process your personal data to meet our legal, regulatory, and/or contractual obligations to provide you with our services. We are obligated to perform due diligence checks of our prospective clients which entail requesting and collecting your personal information, or we will not be able to consider you as a client. That said, we are not obligated to onboard you as a client where we have reviewed your application and documentation and made a reasoned decision not to accept your application. Even if we do not accept your application, your record and the personal data that you provided will be stored with us, in accordance with our regulatory and legal requirements.

We use this information to offer and provide you services, from the first steps in onboarding, through the “kyc” and due diligence stages, setting up client accounts, entering into agreements, and the provision of services. This information is used in accordance with our requirements under different regulations and is used to assess your application to become a client and continuing reviews to ensure that we are able to provide you services.

If you are not yet a client but you have given us your personal data and consent in order for us to reach out, we will use this information to do so with offers relating to our services. If you already are a client, we may contact you in relation to a relevant new service, or to set up our products and services for you, including to provide you with support, boarding, integration, installation, helping you with settings, and other actions which need to be taken to establish or perform our contract with you and providing you with support, optimizing and improving our products and services. If you agree, we will share your data with our third-party partners so that they may offer you their products and services.

We collect the following personal data if you are an employee or candidate:

Information that you provide in your candidate application, sent via our website, LinkedIn, or via a third-party (e.g. a referral by current employee or employment agency) including your CV, resume, other job-related materials such as additional information provided during the interview process, and information you provide to us during the course of your employment (as may be further defined in policies reviewed during employment) .

We use your personal data to determine if you are a good fit for us during the interview process. We will use this information to contact you as a candidate and as an employee, and on occasions, based on information provided by you, we may contact your dependents.

#### Marketing and additional shared data

Communication data and data about your preferences in receiving marketing materials that you send or share with us, or other third parties share with us, whether it be through the contact form on our websites, referral, through email, text, social media messaging, or social media posting, or any other communication.

We use your personal data in accordance only with the purpose for which it was received including to deliver relevant content and advertisements to you and measure or understand the effectiveness of this advertising. For example if you have sent in an email query, we will use personal data to help answer your query;;if you have tagged us in a social media post, we may share on our platforms; or if we received your personal data from a third party, as a referral.

#### Other purposes

We use your personal data received through legitimate means for other purposes, such as, such as our legitimate interest to protect our legal rights in connection with any claims and legal obligation to process your data. We will use this information when we believe that it is necessary to protect our rights, prevent harm of financial loss, protect your safety or the safety of others, investigate fraud or abide by regulations in place to stop fraud, cooperate with law enforcement or government agencies, or in connection with an investigation of suspected or actual fraudulent or illegal activity.

### **SHARING YOUR PERSONAL DATA:**

#### Who We Share Your Data With

Where necessary we will share your personal data with third parties such as:

- Our group of companies.
- Service providers who provide IT, system administration services.
- Professional advisers including lawyers, bankers, auditors, and insurers.
- Services providers who assist with requirements set by authorities and regulatory bodies.
- Government bodies that require us to report processing activities.
- Card Schemes such as Visa, Mastercard, AMEX, etc.
- Service providers and business partners who are involved in providing you services including for example third-parties who provide payment services.

- Other third parties to the extent it is required by a law that is applicable to us, or where you have given your explicit consent.

We will also disclose your personal data to:

- a prospective buyer of our business or a buyer of a substantial number of the shares in our business.
- the police, other lawful enforcement body, regulatory body or court if we are under a duty to disclose or share your personal data, or to protect the rights, property, or safety of ourselves or our group companies, our customers, or others.
- tax authorities, more specifically financial information and transactions, in line with FATCA/ CRS provisions.
- third parties who referred you to us initially and to whom we owe a commission payment as a result of the referral. Where the commission payment is based on transaction volumes, numbers or types of transactions, we share that information with that third party.

We may also transfer your data in the event of a company reorganization, merger, or sale, or to our partners.

All third parties that receive your data must respect the security of your personal data and to treat it in accordance with the Data Protection Regulations. We only allow these third parties to process your personal data for specified purposes and in accordance with our instructions.

We do not sell or otherwise disclose the personal data we collect except as disclosed in this Privacy Policy, or as may be disclosed to you at the time information is collected.

#### Data Transfer Outside of the European Economic Area and the United Kingdom (“EEA and UK”)

Personal data that you send us is stored, processed, and/or transferred to other countries where we have operations or where we engage service providers, and therefore, there are instances where your data is shared, both in and outside, the EEA and UK.

We will only process, store, and/or transfer personal data to and from countries outside the EEA or UK when such country has received an adequacy decision or if there is no adequacy decision, we apply the EU Standard Contractual Clauses (“SCC”) mechanism for when it relates to personal data from the EEA, and for personal data from UK we apply the SCC as they are amended by UK addendum. We may also use other safeguards that are considered as appropriate in accordance with Data Protection Regulations. In addition, we have implemented inter-company agreements that cover data processing between all of our group of companies.

We take measures to ensure that the data processing, storing, and/or transferring comply with the applicable Data Protection Regulations and that your personal data remains protected to the standards specified in this Privacy Policy. In certain circumstances, courts, law enforcement agencies, or security authorities have the right to request access to your personal data.

Whenever we transfer your personal data out of the EEA or UK, we do our best to ensure a similar degree of security of data and only share with a third-party if the following is true:

- Data is being transferred to a country with an adequacy decision or there are appropriate safeguards in place.
- We have made sure that the third-party has equivalent safeguards in place to ensure the protection of your personal data.

In the event that we want to share your personal data with a third-party that is not based in a country with an adequacy decision, and there are no appropriate safeguards in place, we will only share your personal data in accordance with the derogations provided in the relevant Data Protection Regulation.

### **STORING AND RETAINING YOUR PERSONAL DATA**

We securely store your data by maintaining industry approved safeguards designed to protect the personal data provided or collected against accidental, unlawful, or unauthorized destruction, loss, alteration, access, disclosure, or misuse. Such data is also routinely backed up at secure locations in Europe and outside in accordance with standard industry practice. The industry practice specifically related to the Fintech sector is reviewed annually and we update our security measures accordingly. That said, no method of transmission over the Internet, or method of electronic storage, is 100% secure, however, therefore, we cannot guarantee its absolute security. If you have any further questions about privacy or security or have reason to believe your data security has been compromised please contact us immediately by sending an email to: [dpo@shift4.com](mailto:dpo@shift4.com).

We will only retain your personal data for as long as necessary to fulfil the purposes for which it is collected in accordance with our Retention Policy. This includes retaining your data for the purposes of satisfying any legal, accounting, or reporting requirements. When deciding on the applicable retention periods, we consider our regulatory and legal obligations, the processing purposes, nature and sensitivity, potential risk of harm from unauthorized use or disclosure. We also take into consideration best practices applied in the industry.

We take measures to delete or permanently de-identify personal data as required by law or if it is no longer required for the purpose for which it was collected. Certain data relating to transaction records, particularly billing and statement information, may be required to be safeguarded for significant periods of time in accordance with standard tax and accounting practices, or to enable the refund and chargeback requests to be processed on behalf of our customers; additionally such data may be stored to account for requirements relating to financial crime based on the applicable regulations and our company data classification and retention policy.

### **MARKETING**

We would like to send you information about products and services that we think you might be interested in, as well as those of our partner companies. If you have agreed to receive marketing, you may always opt out at a later date. You will receive marketing communications from us if:

- You have asked for information about our services or if you receive or have received our services or you agreed to receive marketing communications; and
- if you have not opted out of receiving such communications.

If relevant, we will request your consent before we share your personal data with any third party for their own marketing purposes. You can ask us or third parties to stop sending you marketing messages at any time.

Occasionally we will send information via email to our clients, unless you have chosen not to receive such communication, including, if we have your consent, from our group companies also, about products, services, and special deals which we think will be of interest to you via our newsletter. You have the right at any time to stop us from contacting you for marketing purposes or giving your data to other members in the Shift4 group. However, please note that we will still send you important administrative messages that are required to provide you with our services.

**If you no longer wish to be contacted for marketing purposes, please contact [marketing\\_eu@shift4.com](mailto:marketing_eu@shift4.com).**

### **YOUR DATA PROTECTION RIGHTS**

Under applicable Data Protection Regulations, you have the following rights with respect to your personal data. We want to make sure you are fully aware of what they are.

**The right to be informed:** You have the right to be informed about the collection and the use of your personal data.

**The right to access:** You have the right to receive copies of your personal data that we have.

**The right to rectification:** You have the right to request that we correct any information you believe to be inaccurate. You also have the right to request that we complete information you believe is incomplete.

**The right to erasure/to be forgotten:** You have the right to request that we erase your personal data. It may be the case that we are required to keep such information in accordance with our legitimate business purposes or to comply with relevant laws, to that extent we will make efforts to limit the processing of your personal data to only what is required.

**The right to restrict processing:** You have the right to request that we restrict the processing of your personal data.

**The right to object to processing:** You have the right to object to our processing of your personal data, under certain conditions.

**The right to data portability:** You have the right to request that we transfer the data that we have collected to another organization, or directly to you, in a structured, commonly used, and readable format.

Additionally, data subjects have the right to not be subject to a decision based solely on automated processing. Please note that we do not apply automated decision processing and if you have any concerns in this regard, you may reach out to us, by making a request [here](#).

In the limited circumstances where you have provided your consent to the collection, processing, and/or transferring of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time, subject to our regulatory and legal requirements.

You will not have to pay a fee to access your personal data. However, we may charge a reasonable fee if your request is clearly unfounded, repetitive, or excessive, or if you refuse to comply with our requests in these circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your legal right to exercise any of your data protection rights. This is a security measure to ensure that personal data is not disclosed to a person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Once we have received notification that you have withdrawn your consent, or you have made a request relating to your rights under Data Protection Regulations, we will respond to your request and will: (i) either confirm that we will no longer process your personal data information for the purpose or purposes you originally agreed to, or (ii) provide our reasoned decision as to why we are unable to grant your request. This can be due to different reasons, such as our legitimate or regulatory basis to retain your personal data.

### **MINORS**

We do not provide services or actively market to children, and we never knowingly ask a child under 13 to divulge personal data. Services and information available on this site or provided following communication with us are NOT INTENDED FOR OR FOR USE BY ANY PERSON UNDER THE AGE OF 18.

Please note that if it comes to our attention through reliable means that you are under 18, we will end all communication and take steps to delete your information.

BY PROVIDING US WITH YOUR DATA, YOU WARRANT TO US THAT YOU ARE OVER 18 YEARS OF AGE.

### **OTHER WEBSITES AND THEIR PRIVACY POLICIES**

Our website contains links to third-party websites, plug-ins and/or applications. By clicking on those links or enabling those connections, it 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 website, we encourage you to read the privacy policy of every website you visit. Our Privacy Policy applies only to our websites.

### **HOW TO CONTACT US, YOUR QUESTIONS, AND COMPLAINTS**

We have appointed a DPO (data protection officer) to oversee compliance with this privacy policy and with the Data Protection Regulations.

You can submit a request relating to your rights mentioned in this policy [here](#)

If you have any additional questions about this privacy policy or how we handle your personal data, you can contact our DPO by sending an email to: [dpo@shift4.com](mailto:dpo@shift4.com)

Please note that, in order to process your request, you may be required to provide additional information, to verify your identity. The information that you provide will be used solely for the purpose of fulfilling your request.

#### **HOW TO CONTACT THE APPROPRIATE AUTHORITY**

We are committed to working with you to obtain a fair resolution of any complaint or concern about privacy. However, if you believe that we have not addressed your concern in a satisfactory manner, you may contact the Office of the Information and Data Protection Commissioner in Malta at:

- Email: [idpc.info@idpc.org.mt](mailto:idpc.info@idpc.org.mt)
- Phone number: (+356) 2328 7100

Or to the Information Commissioner's Office in the United Kingdom here:

- <https://ico.org.uk/make-a-complaint/data-protection-complaints/data-protection-complaints/>