

blue square.

# Data Protection Policy

## Purpose

We're committed to being transparent about how we collect and use personal data and meeting our data protection obligations.

This policy sets out our commitment to data protection, individual rights and our obligations in relation to personal data.

The policy applies to personal data of job applicants, employees (including workers, contractors, volunteers, interns and apprentices) and former employees; as well as any personal data of our customers and any personal data we may handle on their behalf.

Information security and compliance is managed at a group level through our IT, Human Resources (HR) and data analytics teams. Questions about this policy, or requests for further information, should be directed to [gdp@bluesquare.uk.com](mailto:gdp@bluesquare.uk.com)

## Definitions

### **Personal data**

Any information that relates to a living individual who can be identified from that information. Processing personal data refers to any use made of that data – this includes collecting, storing, amending, disclosing or destroying it. This does not include anonymised data.

### **Special categories of personal data**

Information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, and genetic or biometric data.

### **Criminal records data**

Information about an individual's criminal convictions and offences, or relating to criminal allegations and proceedings.

## Data protection principles

We process personal data in accordance with the data protection principles set out in law:

- We process personal data lawfully, fairly and in a transparent manner
- We only collect personal data for specified, explicit and legitimate purposes
- We ensure that personal data held is adequate, relevant and limited to what is necessary for the purposes of processing
- We ensure that the data we hold is accurate, kept up to date and take all reasonable steps to rectify or delete inaccurate data without delay
- We only keep personal data for the duration necessary for processing, and
- We take appropriate measures to ensure that personal data is secure and protected against unauthorised or unlawful processing, accidental loss, destruction or damage

The reasons for processing personal data, how we use it and the legal basis for processing is outlined in our **privacy notices**. We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Where we rely on legitimate interests as the basis for processing data, we carry out assessments to ensure that those interests are balanced against the rights and freedoms of individuals.

Some processing that we carry out may create a risk to privacy. If our data processing results in a high risk to an individual's rights and freedoms, we'll carry out a data protection impact assessment to review the necessity and proportionality of processing. This includes considering the reasons why the processing is needed, the risks for the individuals and the measures that can be put in place to mitigate those risks.

Where we process special categories of personal data or criminal record data to carry out our obligations or exercise our rights in employment law, we do this in accordance with appropriate policies on special categories and criminal records data and we implement

additional safeguards. We do not process special categories of personal data or criminal record data in regards to our customers.

It is important that the personal data we hold about you is accurate and current. You should keep us informed if your personal data changes during your relationship with us. We will update data promptly if an individual tells us their information has changed or is inaccurate.

We keep records of our processing activities in accordance with the requirements of the UK or EU General Data Protection Regulation (**GDPR**) as applicable. Even though we are a UK based data controller, we may be required to comply with both UK GDPR and EU GDPR regimes. UK GDPR will apply to data subjects in the UK and EU GDPR will apply to data subjects in the EU.

## Individual rights

As a data subject, you have rights in relation to your personal data.

### Subject access rights

You have the right to make a subject access request about the data we may hold about you. If you make a request, we'll tell you:

- Whether or not your individual data is processed and why
- The categories of personal data concerned and the source of that data
- Who might have access to that data, including any recipients located outside the United Kingdom (**UK**) or European Economic Area (**EEA**) and the safeguards that apply to such transfers
- For how long your data may be stored, or how that period is decided
- Your rights to rectify or erase the data, or to restrict or object to the processing
- Your right to complain to the Information Commissioner if you think we've failed to comply with your data protection rights, and
- Whether or not we carry out automated decision making and what logic may be used in such decision making

We'll also provide you with a copy of the personal data that's being processed. This will normally be in electronic form if you've made the request electronically, unless you agree otherwise.

We will not usually charge a fee for the original request or disclosure. Although we may charge a reasonable administrative fee to cover the cost of providing you with additional copies of your data.

To make a subject access request, you should contact [gdpr@bluesquare.uk.com](mailto:gdpr@bluesquare.uk.com). We may need to ask for proof of identification before the request can be processed.

We will normally respond to a request within a month of it being made. In some cases, for example, if we've processed a large amount of your data, we may respond within three months of the date of the request. We'll write to you to notify you within a month of your request if this is the case.

If a subject access request is manifestly unfounded or excessive, we reserve the right to either decline to respond to it or to charge a fee to cover the administrative costs of providing the data.

## **Other rights**

You have a number of rights in relation to your personal data. You can ask us to

- Rectify inaccurate data
- Stop processing or erase data if it's no longer necessary for the purposes of processing or by withdrawing your consent
- Stop processing or erase data if your interests override legitimate grounds we may have for processing personal data (where we are relying on our legitimate interests as a reason for processing the data)
- Stop processing or erase the data if the processing is unlawful, and
- Stop processing data for a period, if the data is inaccurate or if there is a dispute about whether or not your interests override legitimate grounds we may have for processing your personal data

To ask us to take any of these steps you should send a request by email to [gdpr@bluesquare.uk.com](mailto:gdpr@bluesquare.uk.com). For further information about your rights under data protection, please visit the Information Commissioner's website [here](#).

## Data security and disclosure

We take the security of personal data seriously. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that the data is not accessible without authorisation and only in the proper performance of relevant duties.

### **Working with Group Companies**

Blue Square Marketing Ltd is part of a group of companies under the Blue Square Group; the group includes OnLive, The Pulse Agency and Creative Monster (**Group Companies**) and shares some staff and functions (for example Central Support functions like HR and finance) between the Group Companies. Data Provided to Blue Square may therefore be shared within the Group Companies and its employees and agents. This will be only so far as is necessary for the proper fulfilment of our services and contractual obligations. The data processing between Group Companies is governed by written agreements and in accordance with this policy and associated privacy notices.

### **Working with third parties**

We may from time to time engage third parties who may process personal data on our behalf in order to provide us with services. For example, for the provision of our HR system or for accountancy or financial services. Details of such processing is set out in our relevant privacy notices.

Where we engage a third party to process personal data on our behalf, the parties do so as data processors on the basis of our written instructions, they are under a duty of confidentiality, and they are obliged to implement technical and organisational measures to ensure the security of data.

This may also apply to third parties to whom we may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this data protection policy

### **Data breaches**

If we discover a breach of personal data that poses a threat to the rights and freedoms of individuals, we will report it to the Information Commissioner within 72 hours of discovery. We will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of the data subject, we will notify you of the breach and provide you with information about the likely consequences and the mitigation measures we've taken.



## International data transfers

We do not normally transfer your data outside of the UK or EEA (depending on which area is applicable to you). If we are required to transfer your data outside of the EEA or UK, we will ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented.

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data. This is known as an “adequacy decision” which is issued by a relevant legal body that deems that the country the data is transferred to has appropriate safeguards in place; or
- We will use specific contract clauses approved for use in the UK or EU which give personal data the same protection it has in the UK or EU. These are known as International Data Transfer Agreements for data transfers between the UK or EU and other countries.

## Training

We are committed to our data protection obligations. When we provide our services to our customers, our employees sometimes have need to access to employee or customer personal data. We require all new hires to the business to complete training about their data protection responsibilities as part of our induction processes.

Those in roles that require regular access to personal data, who are responsible for implementing this policy, or responding to subject access requests under this policy will receive additional training to help them understand their duties and the best ways these can be complied with.

## Retention of records

We follow recommendations made by the Information Commissioners Office on the retention of records. We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for longer in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

By law we have to keep basic information about customers for up to six years for tax purposes. The retention period for HR records is set out in our employee privacy notice.

In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use that information indefinitely without further notice to you.

## Changes to this policy

We keep this policy under regular review and reserve the right to update it from time to time. We will publish any changes and notify you when we make any substantial updates about the

## Version Control

▪ Document version	V4.0
▪ Reason for Document Update	Changed the ref to SSC's to international data transfer agreements
▪ Next Review Date	October 2023 <i>or as required - subject to operational amendments</i>

## Revision History

Version	Changes	Changes By	Revision Date
1.0	First Live Release	Charlotte Comer / Ian Cannonier	22 May 18
1.1	Template changed/ Compliance Manager update	Daniel Troaca	26 Nov 18
2.0	Annual Review, re-version and publish	Alan Duncan	6 Sep 19
3.0	Legal update following establishment of group companies	Nick White	1 Oct 21
4.0	Changed the ref to SSC's to international data transfer agreements	Matt Harman	03/01/2023