

Introduction to Our Data Protection Policy Portfolio

Information, policies and procedures for compliance with “The General Data Protection Regulation”

About Us

Where reference is made to terms such as “our”, “we” and “the company”:

Company Name: Bluesock.com Limited.

Where reference is made to our “Data Protection Officer”:

Our nominated Data protection officer is: Mike Wainwright

Where reference is made to our website:

Our Website is defined as: www.bluesock.com

For the definition of other terms in our policy please refer to the “General Definitions” document.

General Statement of Principles

We value and respect the privacy of your data and we limit our processing of your data for our normal business operations.

We will not hold your data longer than we need, to meet our legal and financial obligations.

We will not transfer or sell your details to anyone else without your informed and express consent.

We will take due diligence and all reasonable measures to keep your data secure and private.

All relevant business practices are carried out in line with these principles and policies

Background

The General Data Protection Regulation (GDPR) is based around the principles of handling of personal data. We must comply with all six principles as a business; otherwise we’ll be in breach of the GDPR. We understand that the principles give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

Third Parties

Contracts between the company and any party whether employees, suppliers, data processors, other third parties or authorised individual are subject to these policies.

Specifically, where it is necessary to share any personal data with a third party (such as an accountant, payroll provider, pension authority, sub-contractor, supplier or data processor) we will undertake our best endeavour to ensure third-party compliance with our policies.

During the procurement and renewals of contracts we will undertake to ensure that the party is made aware of our policies and their requirement to act accordingly.

Implementation

Please see our other policy documents in this portfolio, available at our registered offices and where appropriate published on our website.

Policy Documents include:

- Our Cookie Policy
- Our Data Privacy Notice for Customers and Supplier
- Our Data Privacy Notice for Employees
- Our Data Breach Policy
- Our Staff Data Protection Training Policy
- Our Subject Access Request Policy
- Our Website Acceptable Use Policy
- Our Website Terms of Use

Additional Documents include:

- General Definitions

Any additional Documents applicable will be included in the

- Addendum and Revisions Section

Foundation Principles

Our policies have been formed around the following:

GDPR: 8 rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification

4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>

GDPR: 5 protection principles

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

1) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

i) at least one of the conditions in Schedule 2 is met,
<http://www.legislation.gov.uk/ukpga/1998/29/contents#sch2>

ii) and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
<http://www.legislation.gov.uk/ukpga/1998/29/contents#sch3>

2) Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4) Personal data shall be accurate and, where necessary, kept up to date.

5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6) Personal data shall be processed in accordance with the rights of data subjects under this Act.

7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.