INSIGHT REPORT LTD (IRL)

Data Protection and Governance

1. Our Core Principles

Our initial purpose in creating Credscope is to enable people without a credit history to get an opportunity to access the products and services they need fairly and ethically, in order to have a positive impact on their financial wellbeing. We work with businesses and social enterprises who provide relevant products and services to consumers seeking those products and services.

To achieve this purpose, we will act with integrity in everything that we do, seeking to obtain maximum benefit for people and planet, whilst treating our customers fairly and with respect. This means that we will put our customers' interests and benefit at the centre of all that we do.

2. Governance

We have appointed board members at the highest level of our business to challenge, advise and ensure that our business maintains our stated purpose in an ethical manner always. The non-executive director lead on our data accountability and governance is our Compliance Director.

Principles

Our operations are carried out in accordance with the eight principles of UK Data Protection Act (DPA), and the EU's General Data Protection Regulation (GDPR) 2016, which come into effect in 2018. Other policies and procedures include our Treating Customers Fairly, Privacy, and Terms and Conditions of Use.

The principles of the DPA as adopted by IRL are:

1. Personal data shall be processed fairly and lawfully

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.

The principles of the GDPR are similar to those in the DPA, with added detail at certain points, and a new accountability governance requirement. This document sets out key details of our approach to data accountability and governance.

Name and details of our organisation

Insight Report Ltd

Purposes of processing

Credit Referencing service. Our processing is based on the explicit consent of the data subject, and is necessary to protect the vital interests of a data subject or another person, namely the service provider.

Description of the categories of individuals and categories of personal data

Individuals with little or no credit history: this category includes young professionals, expatriates, tenants, financially excluded people, and recent graduates.

Personal data includes: name and address, rental information, other regular payments, as per attached form in Appendix 1.

Categories of recipients of personal data

Lenders

Service providers

Details of transfers to third countries including documentation of the transfer mechanism safeguards in place

We do not transfer data outside the UK.

Retention schedules

We will retain records, with explicit consent, as required by customer actions, operations and legal requirements. The customer has the right to withdraw consent, make corrections, and to be "forgotten", which will be implemented in line with legal requirements operating at the time.

Retention will be reviewed in accordance with customer requests, operational and legal requirements. We will securely delete information that is no longer needed for these purposes, and update, archive or securely delete out of date information.

Breach Reporting

The ICO defines a personal data breach as a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

What to report	Who	When
Data loss, unauthorised access, disclosure Why: can result in financial loss, loss of privacy, disadvantage	Data Protection Officer	Within 72 hours
The nature of the personal data breach including, where possible: • the categories and approximate number of individuals concerned;	Data Protection Officer	Within 72 hours

• the categories and approximate number of personal data records concerned;		
The name and contact details of the data protection officer or other contact point where more information can be obtained;	Data Protection Officer	
A description of the likely consequences of the personal data breach	Data Protection Officer	
A description of the measures taken, or proposed to be taken, to deal with the breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.	Data Protection Officer	

Business continuity

The purpose of our business continuity plan is to ensure that we can continue to function and meet our regulatory obligations in the event of unforeseen interruption. We will regularly update and test these arrangements to ensure their effectiveness.