

NAME OF ORGANISATION:	Resilient Business Systems Limited
DATA PROTECTION OFFICER(S):	Andrew Read – Managing Director Michelle Read – Company Secretary
DATE OF POLICY IMPLEMENTATION:	22 May 2018
DATE OF POLICY REVIEW:	22 May 2021 (or before if legally required)

Glossary

“Individual”	For the purpose of this document, this can be an individual or a customer business.
“SAR”	Subject Access Request
“GDPR”	General Data Protection Regulation

Purpose of Policy

Individuals (for the purpose of this policy this includes Customers) have the right under the General Data Protection Regulation (GDPR) to have access to their personal records that are held by Resilient Business Systems Limited (RBS). This is known as a ‘Subject Access Request’ (SAR). Requests may be received from members of staff or customers. This will include information held both electronically and manually and will therefore include personal information recorded within electronic systems, spreadsheets, databases or word documents.

Anyone making such a request is entitled to be given a description of the information held, what it is used for, who might use it, who it may be passed on to, where the information was gathered from. Under GDPR individuals must also be provided with information on the expected retention periods of the information held, the right to request rectification or erasure of processing or raise an objection to the processing altogether.

This policy is to be read in conjunction with our Data Protection and Privacy Policy.

What is a Subject Access Request (SAR)

A SAR is simply a written request made by or on behalf of an individual for the information about them, which is held by RBS. The GDPR entitles all individuals to make requests for their own personal data. An individual is not entitled to information relating to other individuals (unless they are acting on behalf of that individual).

The request does not have to be in any particular form other than in writing, nor does it have to include the words ‘subject access’ or make any reference to the GDPR. A SAR may be a valid request even if it refers to other legislation, such as the Freedom of Information Act 2000 (FOIA) and should therefore

be treated as a SAR in the normal way. The applicant must be informed of how the application is being dealt and under which legislation.

Subject access is most often used by individuals who want to see a copy of the information an organisation holds about them.

However, subject access goes further than this and an individual is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the personal data; and
- given details of the source of the data (where this is available).

Personal data is information that relates to an individual who can be identified either directly or indirectly and includes any expression of opinion about the individual and any indication of the intentions of the information holder or any other person in respect of the individual. Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR.

Processing a SAR

Upon receiving a SAR, the staff member must pass this immediately to a Data Protection Officer. The Data Protection Officer will then determine if the person who has submitted the SAR has the right to the data being requested, especially if it is a SAR on behalf of a customer business.

If the SAR is in respect of Crime and Taxation (eg from the Police or HMRC), a formal documented request signed by a senior officer from the relevant authority is required before proceeding with the request. This request must make it clear the purpose for the request and that by not receiving the information would prejudice any investigation.

Any Court Order requiring the supply of personal information about an individual must be complied with.

Throughout the process, the Data Protection Officer must update the SAR spreadsheet which details:

- Date SAR received
- Date response due (30 calendar days from the date of receipt)
- The Applicant's details
- The information requested
- Exemptions applied in respect of information not disclosed
- Details of information disclosed and the format they were supplied in
- Date information supplied

The Data Protection Officer will then collate together the required information.

If the information collated contains any information about any other individuals or third parties, the Data Protection Officer must consider:

- Is it possible to comply with the request without revealing information that relates to the third party?
- Can consent be obtained from the third party to the disclosure?
- Is it reasonable, considering the circumstances, to comply with the request without the consent of the third party?
- Duty of confidence owed to the third party
- Any express refusals of consent from the third party

If the information requested is held by RBS and exemptions apply then the Data Protection Officer must determine if the applicant is informed that the data is held but that it is exempt from disclosure or if a reply is provided stating that no relevant information is held. It may then be necessary to reconsider this decision should a subsequent application be made and circumstances around the use of exemptions has altered.

If the information contains complex terminology the Data Protection Officer must ensure that this terminology is explained in such a way that the information can be understood in lay terms.

Responding to a SAR

Where it is ascertained that no information is held about the individual concerned, the applicant must be informed of this fact.

A copy of the information must be sent out securely in an agreed format. For example, if an email is to be sent containing a word, excel or pdf document, the document must be password protected and the password sent separately. If the data is in multiple formats, then a OneDrive shared folder may be used but again this must be password protected.

Under no circumstances should original documents be sent to the applicant.