

Data Protection Policy

RSL Project Solutions Ltd must ensure it collects, processes and maintains personal and sensitive personal information (hardcopy or electronic) on individuals; including employees and third parties, in accordance with the General Data Protection Regulation (GDPR) and other applicable laws.

Personal information means any information which, by itself or when combined with other information that RSL Project Solutions Ltd may hold/obtain, can identify a natural person; in particular by reference to an identifier such as a name, email address, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Personal sensitive information is a subset of personal information and means personal information related to racial or ethnic origins, religious beliefs, political opinions, trade union memberships, physical or mental health or condition, and other medical information including biometric and genetic data, or sexual life or preferences. In some instances, sensitive personal information may also include criminal allegations offences or convictions, precise geolocation information, financial and bank account numbers or unique government issued social security numbers, driver's license, and passport numbers.

Third Party information includes personal and / or sensitive personal information which we routinely collect on our customers, suppliers and partners as well as information that we are required to hold on their behalf.

GDPR is applicable across the European Economic Area ("EEA"), to companies that offer goods and services to, or monitor individuals in, the European Union ("EU") requiring the collection and handling of personal and/or sensitive data which will be subject to GDPR and possibly other applicable laws.

To be compliant with GDPR RSL Project Solutions must

Retain evidence of what personal information it is collecting, handling and maintaining on its employees and third parties. All new collection and handling of personal information must be approved by the Data Protection Officer who will determine the purpose for collecting and handling the personal information and whether RSL Project Solutions will need to obtain consent prior to processing the personal information. This must be captured in a Privacy Impact Assessment (PIA).

Determine where it is relying on consent from third parties to process their personal information and the timescales to refresh their consent; e.g. every 12 months etc. The Data Protection Officer will evaluate whether this is required from any third parties given the purpose for collecting and handling the personal information. Specifically:

- Consent to continue to hold and maintain third party information, such as a personal CV, must be obtained from the individual annually; confirming that we can continue to

hold the data and that it is accurate. Evidence of this should be retained for the period we are processing and/or retaining the personal information for.

Should a third party request to withdraw their consent for RSL Project Solutions Ltd to continue to retain and/or process their personal information they should be directed to our Data Privacy Notice or to contact the Managing Director.

Maintain an effective data protection regime - to demonstrate that RSL Project Solutions Ltd is only retaining the personal information that it needs; that it has consent where required, and that personal information is being kept up-to-date.

Provide transparency of employees' personal information and ensure that they have appropriate means to update the accuracy of their personal information. Employees must be provided with an opportunity to review the personal information being held on them at least annually.

Ensure that our systems and tools allow for the new rights related to personal information that we are maintaining, namely the right to be "forgotten"; to "restrict" the handling of personal information; and to "data portability" requiring that in certain circumstances personal information may not be able to be collected or handled and/or may need to be deleted or passed directly to another external third party. Any requests to be forgotten and/or for erasure and/or for restricted handling will need to be approved by the Data Protection Officer who will determine whether the request conflicts with and any of RSL Project Solutions Ltd's rights to continue collecting and handling the personal information, e.g. a legal requirement.

Conduct a Privacy Impact Assessment (PIA) to understand the risk associated with processing personal information prior to engaging in any activity. A PIA must be completed when:

- Engaging with a Third Party who will collecting and/or processing data on our behalf
- procuring or developing an IT Tool which will collect any personal data
- engaging with customers on a business sales opportunity
- engaging on any monitoring activity on employees and/or third parties - any monitoring will need to be approved by the Managing Director

The outcome of the PIA should be retained as evidence. All completed PIAs must be approved by the Data Protection Officer.

Conduct appropriate due diligence on any supplier who will act as a third party processor for collecting and handling personal information, and, continue to monitor those suppliers to ensure their ongoing compliance

Determine the appropriateness of all transfers of data, either to Third Parties based either inside or outside the EEA. All transfers of data to third parties must be authorised by the Data Protection Officer who will determine whether this is feasible and implement any mitigations to reduce the risk to RSL Project Solutions Ltd.

Complete all legal requests such as Subject Access Requests (SARs) within their statutory deadlines - the Information Commissioner requires all SARs to be responded to within 30 days.

Disclose any breaches of the regulation to the Information Commissioner within 72 hours of identification of the breach occurring, and in certain circumstances to the affected individuals. Any breaches must be reported immediately to the Data Protection Officer, who will liaise with the supervisory authority and determine whether individuals should be informed of the breach.

Publish a Privacy Statement which informs individuals (employees and third parties) how their personal information will be collected and handled, the purposes for which the personal information has been collected and RSL Project Solutions Ltd's commitment to maintain it and store the personal information in a compliant manner.

Ensure that personal information (employee and/or third party) is not shared with any other third party without the express consent of the natural person to whom the personal information relates.

What if personal data is disclosed?

Every disclosure/transfer of personal information outside of RSL Project Solutions Ltd must be recorded. This record must be retained with the personal information for as long as that personal information is maintained.

What happens in response to a Subject Access Request (SAR)?

On request in writing (including fax and email) an individual whose identity has been adequately verified, and who has identified the nature of the personal information they wish to access, is entitled (subject to disclosure exemptions) to have communicated to them in intelligible form:

- Their personal information as held; and
- any information available to RSL Project Solutions Ltd as to the source of this personal information; and
- to which recipients this personal information has been disclosed.

On receipt of a request from any individual for disclosure of all or some of their personal information the Data Protection Officer will log this request on the data protection SAR Register. The point of contact is responsible for ensuring that an appropriate response is sent within the statutory 30 calendar- day timescale.