

Data Protection Impact Assessment (DPIA) Policy Statement

Sign In App (together with its affiliated companies) has a legal obligation under the Data Protection Act 2018, UK GDPR and the EU GDPR to perform a Data Protection Impact Assessment (DPIA) for high risk processing activities.

Aim

Our aim is to ensure that 'Privacy by Design and Default' are embedded into our processes and that conducting a DPIA for activities that relate to processing of personal data will help to identify any risks, apply appropriate solutions and mitigating actions where processing is deemed likely to cause high risk to one or more individuals.

What types of processing automatically require a DPIA?

- Systematic and extensive profiling with significant effects
- Large scale use of sensitive data
- Public monitoring

What other factors might indicate likely high risk?

- Evaluation or scoring.
- Automated decision-making with legal or similar significant effects.
- Systematic monitoring.
- Sensitive data or data of a highly personal nature.
- Data processed on a large scale.
- Matching or combining datasets.
- Data concerning vulnerable data subjects.
- Innovative use or applying new technological or organisational solutions.
- Preventing data subjects from exercising a right or using a service or contract.

Policy Review Statement

- This policy statement may be reviewed at any time and at the request of either staff or management, but will automatically be reviewed 3 years from the initial approval and thereafter on a triennial basis unless organisational changes, legislation, guidance or non-compliance prompt an earlier review.

Our full Data Protection Impact Assessment Policy is available on request.

For further information about Sign In App's compliance with data protection law, please contact:

Governance, Risk and Compliance Team
Email: privacy@signinsolutions.com

Alternatively you can contact the information Commissioner's Office Directly on 0303 123 1113 or at <https://ico.org.uk/>