

Data Protection Policy

The rights of individuals about whom information is held are as following:

- The right to be informed about the collection and use of their personal data
- The right to access their personal data (commonly referred to as subject access)
- The right to have inaccurate personal data rectified, or completed if it is incomplete
- The right to have personal data erased when the individual objects to the processing of their data under legitimate interests basis and there is no overriding legitimate interest to continue this processing
- The right to restrict processing
- The right to object to the processing of their personal data in certain circumstances (eg. for direct marketing)
- The right not to be subject to automated decision-making including profiling

Our Data Protection Policy is our overarching Privacy Notice and will give information about how, why and when we collect and use personal information and what we might do with it:

What personal data we hold?	Where it came from?	Why we collect this data?	How we store the data	How long we keep it for?	Who we share it with?	Lawful basis
Staff's name	Personally provided	Service delivery	Electronically and on paper	6 years	Clients, SIA, Police, government departments	Legitimate interests
Staff's address	Personally provided	Service delivery	Electronically and on paper	6 years	Clients, SIA, Police, government departments	Legitimate interests
Staff's email address	Personally provided	Service delivery	Electronically and on paper	6 years	Clients, SIA, Police, government departments	Legitimate interests

What personal data we hold?	Where it came from?	Why we collect this data?	How we store the data	How long we keep it for?	Who we share it with?	Lawful basis
Staff's phone number	Personally provided	Service delivery	Electronically and on paper	6 years	Clients, SIA, Police, government departments	Legitimate interests
Staff's date of birth	Personally provided	Service delivery	Electronically and on paper	6 years	Clients, SIA, Police, government departments	Legitimate interests
Staff's right to work	Personally provided	Service delivery	Electronically and on paper	6 years	Clients, SIA, Police, government departments	Legal obligation
Staff's SIA Door Supervisor licence	Personally provided	Service delivery	Electronically and on paper	6 years	Clients, SIA, Police, government departments	Legitimate interests
Staff's bank details	Personally provided	Service delivery	Electronically and on paper	6 years	-	Performance of a contract
Staff's NINO	Personally provided	Service delivery	Electronically and on paper	6 years	HMRC, DWP	Legal obligation

Secure Frontline Services take responsibility for complying with the relevant Data Protection legislation at the highest management level and throughout our organisation:

- The person responsible for data protection compliance within the organisation is the Director.
- Everyone managing and handling personal information is appropriately trained to do so and understands that they are contractually responsible for following good data protection practice.
- We provide individuals with privacy information at the time we collect personal data
- We adopt a 'data protection by design and default' approach, putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations.
- We maintain a documentation of your processing activities, including any subject access request verbally or in writing
- We consider carrying out a Data Protection Impact Assessment (DPIA) before any type of processing which is likely to result in a high risk to individuals' interests.



- In the event that a personal data breach occurs (accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data), we will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we will notify Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we will also inform those individuals without undue delay.
- We will be keeping a record of any personal data breaches, regardless of being or not being notified to ICO.
- If an individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing, we will erase their data and inform of the erasure any third party that we have disclosed their personal data to.
- Any further change to our Data Protection Policy will be communicated to all individuals about whom information is held by way of an e-mail. Continuing the use of our services after we publish or send a notice about our changes to this Privacy Policy means that the collection, use and sharing of your personal data is subject to the updated Privacy Policy.