



Protectas

Protectas Digital Services

Details of processing and list of sub-processors

Date of the last update: 12/01/2024

Protectas has strong values, and we share a great sense of responsibility towards our clients, employees, and the communities in which we operate. Integrity is one of Protectas' core values, and data privacy is paramount to preserve and respect your integrity. To further our transparent processing of personal data, Protectas provides you with this document.

This document details the processing and provides a list that identifies **the sub-processors authorized to process personal data carried out under the instructions of and on behalf of the client** for all **Digital Services, including MyProtectas services and Risk Intelligence Center Services (RICS)** on behalf of the client.

Please note that this document does not cover personal data processing performed by Protectas being data controller for such processing. Any Digital Services where Protectas does not process personal data on behalf of the client are excluded from this document.

Prior to engaging any sub-processor, Protectas ensures that such sub-processor will implement adequate technical and organizational security measures to ensure that the personal data processed by the sub-processor is sufficiently protected. In the event the sub-processor processes personal data in a third country, Protectas ensures that the relevant personal data transfer mechanism is implemented.



1. MyProtectas services

Please note that note that this section does not include the following MyProtectas services, as these services do not include any processing of personal data by Protectas on behalf of the client:

- MyProtectas Remote Services,
- MyProtectas Risk Prediction Essential,
- MyProtectas Risk Intelligence Awareness.

1.1. List of sub-processors for MyProtectas services

Entity name	Registered address	Sub-processing activity	Location of data processing	Transfer mechanism outside EEA	MyProtectas service	
					Mobile Guard Reporting	Guarding
Securitas Intelligent Services AB	P.O. Box 12307 Lindhagensplan 70 102 28 Stockholm, Sweden	Provider of the service, including user experience and service development	Sweden	N/A	Yes	Yes
Securitas Intelligent Services Poland Sp. z.o.o.	ul. Postępu 6 02-676 Warsaw Poland	Application monitoring and support	Poland	N/A	Yes	Yes
Microsoft Ireland Operations Limited	70 Sir John Rogerson's Quay, Dublin 2, Dublin, D02R296 Ireland	Provider of infrastructure services (Microsoft Azure)	Ireland and the Netherlands	N/A	Yes	Yes



1.2. Details of processing for MyProtectas services

1.2.1. **MyProtectas Mobile Guard Reporting** is a digital product to show guarding information. By using MyProtectas Mobile Guard Reporting the client's end-users are provided with digital access to one, a few or all the sites connected to the client. Through MyProtectas Mobile Guard Reporting the end-users can access callout and beat reporting data. End-users may access the interface by using a webpage or an application.

Description and purpose	Duration of processing and retention times	Type of personal data	Categories of data subjects
To deliver the MyProtectas Mobile Guard Reporting service to the client in accordance with the terms. This service makes it possible for users to consume guard reports aggregated and in detail. Additionally, end-user may add client-specific content such as comments. There might be personal data in comments.	The information is processed for as long as the service is active and in accordance with legal requirements. Information contained within guard reports is stored for 18 months, attached images are stored for 6 months.	Information contained within guard reports or other client specific content.	Individuals that are mentioned in guard reports or other client-specific content such comments entered by end-users.

1.2.2. **MyProtectas Guarding** is a digital service that allows clients' end-users to access guard reports and insights in one digital interface and easily understand what happened where. It allows clients to engage in security proactively. Insights are presented on one single global platform, based on data from events on site(s). Guarding allows the client and its end-users to view detailed reports on events and incidents and aggregated statistics. Guarding also allows end-users to work collaboratively with colleagues by sharing and commenting reports.

Description and purpose	Duration of processing and retention times	Type of personal data	Categories of data subjects
To deliver MyProtectas Guarding service to the client in accordance with the terms. This service makes it possible for users to consume guard reports aggregated and in detail. Additionally, end-user may add client-specific content such as comments. There might be personal data in comments.	The information is processed for as long as the service is active and in accordance with legal requirements. Information contained within guard reports is stored for 18 months, attached images are stored for 6 months.	Information contained within guard reports or other client specific content.	Individuals that are mentioned in guard reports or other client-specific content such comments entered by end-users.



2. RICS – Risk Intelligence Center Services

Please note that this section does not include the service levels RIC Bronze or RIC Silver, as these services do not include any processing of personal data by Protectas on behalf of the client.

2.1. List of sub-processors

Entity name	Registered address	Sub-processing activity	Location of data processing	Transfer mechanism outside EEA	Risk Intelligence Center Services		
					Gold	RFI	Platinum
Securitas Intelligent Services AB	P.O. Box 12307 Lindhagensplan 70 102 28 Stockholm, Sweden	Provider of the service	Sweden	N/A	Yes	Yes	Yes
Securitas Security Services (UK) Limited	24 Old Queen Street, London, United Kingdom, SW1H 9HP	Performance of the RICS as ordered by the client	UK	Adequacy decision	Yes	Yes	Yes
Social Navigator, Inc.	155 Chain Lake Drive unit 8 Halifax NS B3S 1B3 Canada	Provision of the underlying platform enabling the delivery of RICS. The platform is used for collecting information which in turn might be included in the reports sent to the client.	Canada	Adequacy decision	Yes	Yes	Yes



Microsoft Ireland Operations Limited	70 Sir John Rogerson's Quay, Dublin 2, Dublin, D02R296 Ireland	Provider of Microsoft services, i.e. application support and hosting of Microsoft 365	Ireland and the Netherlands	N/A	Yes	Yes	Yes, if not decided otherwise
---	--	---	-----------------------------	-----	-----	-----	-------------------------------

2.2. Details of processing for Risk Intelligence Center Services

RIC Gold and RIC Request for Intelligence (RFI) – At Gold level, the recurring risk intelligence reports are customized based on the client's demands and input. The client may request bespoke reports called Request for Intelligence (RFI) such as specific open-source intelligence reports for threat or defensive purposes. For all personal data required to draft the reports, the client is data controller as the reports (whether recurring or not) are drafted based on the requirements provided by the client who has a decision-making role. Additionally, the client may provide additional information, including personal data which will be used to prepare the report.

RIC Platinum – At Platinum level, an embedded analyst is offered to the client. The analyst could be based at the client's premises or elsewhere and will remain supported by the tools and expertise of the rest of the Risk Intelligence Center. The client is considered data controller as it will determine the scope and purpose of any data processing conducted by the analyst and may impact the means of such processing.

Description and purpose	Duration of processing and retention times	Type of personal data	Categories of data subjects
To deliver the service requested by the client. Processing of personal data collected through publicly available sources (or provided by the client) in line with the instructions from the client necessary to provide services to the client through reports, embedded analyst services or specific open-source intelligence reports for defensive or threat purposes.	For personal data included in the reports, manual removal following send-out (retention time for RFI reports adjustable in line with client needs). For embedded analyst services, varying depending on the nature of the data and the assignment. At the latest following termination of the analyst services, but data might be deleted throughout the assignment depending on client's instructions.	All personal data included in the reports, which could be any type of personal data discovered and communicated to the client (both publicly available and data provided by the client), including names, contact details, social media accounts linked to the data subjects and related posts and images.	Individuals employed by or representing the client and any individual appearing in reports (could be public figures but also employees or external people chosen by the client) within the scope of the service, including individuals who may pose potential threat to the client, as determined by the client.