Privasee

# SEAL Scope: SecureAppbox/SecureMailbox service

## A Data Protection Impact Assessment (DPIA) was conducted on the on the SecureAppbox/SecureMailbox service in January 2018 which lead to the award of the Privasee SEAL.

This is the SEAL report providing scope of the award. Privacy best practices used were: Privasee's 7-step Agile DPIA, and Privacy by Design principles. A DPIA was triggered in January 2018 due to expiry of SEAL issued in 2016. Any privacy risks identified at the ASSESS & COMPLY phase were effectively and immediately remediated by SecureAppbox AB which lead to the award of the SEAL on 1st February 2018.

Privasee's unique 7-step Agile DPIA was used in the assessment, output are privacy risks, i.e. risks to the rights and freedoms of the individual. By February 2018 the client implemented privacy remediations into the SecureAppbox service, and the SEAL was renewed.

### Privacy Risks

Privacy risks identified as 'problematic data actions' with potential consequences of 'harm to the data subject' during the ASSESS phase were minor, have been completely or adequately remediated to the satisfaction of the Assessor which has lead to the renewal of the SEAL on 01 February 2018.

| 1 | 2 | 3 |
|---|---|---|
| **ASSESS & COMPLY** | **ACT** | **SEAL** |
| Privacy risks, personal-data-flows, privacy policies, adherence with privacy principles | Client has 3 months to implement privacy required remediations, the output from step (1) | Awarded when evidence of privacy remediations have been *acted* upon |

**What is GDPR?**
This report is about compliance with the EU GDPR best practices in privacy.

**What is the 'SEAL'**
It is evidence the holder adheres to privacy best practices and is a suitable custodian of personal data

The SecureAppbox / SecureMailbox service has been SEALed

Renewal on 1st February 2020

## Privacy by Design (PbD) principles

| Principles | SecureAppbox/Mailbox service |
|---|---|
| **Proactive not Reactive; Preventative not Remedial** | An external technical security report (BitSec) was conducted on the application/service. |
| **Privacy as a Default Setting** | By users are hidden to their contacts, with the option to make visible at the click of a mouse, this is one of many examples. |
| **Privacy Embedded into Design** | Privacy settings are provided in the design of the services. |
| **Full Functionality - Positive-Sum, not Zero-Sum** | There is no sacrifice of usability in the name of privacy and security. The service is easy to access and use. |
| **End-to-End Security - Full Lifecycle Protection** | Security is built into the service from cradle to grave for personal data and mailbox contents. The SecureMailbox triggers by default options on SEND e.g. "for your eyes only", "destroy after reading".<br>The encryption key is owned by the user which means SecureAppbox does not have access to contents of the service. |
| **Visibility and Transparency - Keep it Open** | A clearly written privacy policy can be found linked from the home pages of the services and within the application.<br>Users have direct access (2-factor authentication) to modify personal data stored within the service. |
| **Respect for User Privacy - Keep it User-Centric** | The user controls their: personal data.<br>Users have 'self-service' access to their personal data.<br>The user can request that their personal data is deleted at any time. |

## Data Protection Impact Assessment

| DPIA Findings | |
|---|---|
| **DPIA Scope** | Personal data stored in SecureMailbox, SecureAppBox service, which are one and the same. |
| **Purpose necessity** | Purpose of collection is to purely provide a service. |
| **Collection points** | Collection of personal data is aligned to the specific purpose and all collection has a legal basis for processing (Art 6). |
| **Processors and accountability** | SecureAppbox AB is a processor in the provision of the service to controllers.<br>SecureAppbox AB is a controller in the collection of personal data required in order to ensure secure and authorised access to the admin functions in the application.<br>SecureAppbox AB has engaged processors in order to provide the service: (1) Amazon AWS for infrastructure/storage, and (2) DIBS Payment Services AB for credit card payments. |
| **Use, retention and disclosure** | Use is aligned with purpose.<br>Personal data is stored for as long as the account is active.<br>Deactivated accounts are removed after 8 weeks in the SecureMailbox account.<br>Personal data is not disclosed to 3rd parties. |
| **Legal basis for processing** | Article 6 (a) consent, and (b) contract were identified. There was also a (c) legal obligation, on financial data, security analytics. |


SecureAppbox / SecureMailbox Service (https://www.secureappbox.com/ www.securemailbox.com/)
Valid until 01 February 2020