Privasee

SEAL Scope: SecureMailbox service

This is a FINAL report on compliance with the upcoming EU General Data Protection Regulation (GDPR) issued to the Data Controller, SecureMailbox AB for their SecureMailbox service.

This is the supporting report providing scope of the award and service factors assessed against the GDPR. Privacy best practices used were: ISO/IEC 29100 Privacy Framework standard, and Privacy by Design principles. A Privacy Impact Assessment (PIA) was conducted on the target service in October 2015. Between November 2015 and January 2016, the client implemented privacy remediations into the SecureMailbox service in order to earn the award of the SEAL.

Privacy Risks

The type of personal data collected is minimal and not sensitive. The risk assessment conducted was rudimentary and aligned to the low risk threshold for the project. Privacy risks identified as 'problematic data actions' with potential consequences of 'harm to the data subject' during the ASSESS phase have been completely or adequately remediated to the satisfaction of the Assessor which has lead to the award of the SEAL on 01 February 2016.

Risks identified outside of the accountability boundaries of the Data Controller, was that users may include personal and/or sensitive data in the message contents. Privacy by Design (PbD) Principles embedded into the service give the user ample control over not only their personal data, but data lifecycle phases on the contents of messages including auto destruction options under user Settings.

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 General Data Protection Regulation

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

ASSESS, COMPLY, ACT, SEAL
The SecureMailbox service has been SEALed*

*Renewal on 01 January 2018

Personal Data Lifecycle (PDLC)

There is a single data collection point from within the application itself, when a user creates/activates an account. The personal data collected is controlled by the user of the service via the Settings option in the application. The user has the choice to delete their account at any time.

There are two use-cases for data collection: 1) when the user creates an account for themselves; and, 2) when the account creation is triggered by a user that sends a message to a non-registered user of the service.

Privacy by Design (PbD) principles

Principles	SecureMailbox service
Proactive not Reactive; Preventative not Remedial	Privacy 'future-proofed' by compliance with the GDPR; including Privacy by Design principles.
Privacy as a Default Setting	By default phone numbers of 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 principles as defined in the ISO/IEC 29100 Privacy Framework standard are built into the service.
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.
Visibility and Transparency - Keep it Open	Built into the service are accessible links to privacy policy, ToS, etc.
Respect for User Privacy - Keep it User-Centric	The user controls their: personal data, their mailbox, and even if selected, on messages that are sent.

ISO/IEC 29100 Privacy Framework

PRIVACY Control	SecureMailbox service
Consent and choice	Explicit' consent on account creation, 'unambiguous' consent on privacy policy updates.
Purpose legitimacy and specification	Purpose of collection is to purely provide a service.
Collection limitation	Collection aligned to the specific purpose.
Data minimisation	Personal data is not duplicated and/or distributed without consent of the data subject. Deleted accounts are securely erased from media.
Use, retention and disclosure limitation	Use is aligned with purpose. All data relating to the service is stored securely on Amazon AWS cloud servers in Ireland, Europe and will not be disclosures unless required by law.
Accuracy and quality	Users have direct access (2-factor authentication) to modify personal data stored within the service.
Openness, transparency and notice	A clearly written privacy policy can be found linked from the Securemailbox home page and within the application.
Individual participation and access	Users have 'self-service' access to their personal data.
Accountability	N/A until 2018 when the EU Data Protection Commission reporting authority is implemented.
Information security	The mailbox is stored in the Amazon AWS cloud. This has been assessed against recognised security accreditations, e.g. ISO27001, SAS70 Type II, PCI-DSS. An external technical security report (BitSec) was conducted on the application/service.
Privacy compliance	PUL and GDPR

Privasee SEAL

SecureMailbox Service (https://my.securemailbox.com/)
Valid until 01 January 2018

Related evidence:
1. Evidence of Privasee SEAL at http://privasee.se/privasee-seal/.
2. Privasee SEAL - Evidence of Compliance - GDPR (Scope: SecureMailbox-Service)