Privasee SEAL

SCOPE – SECUREMAILBOX SERVICE

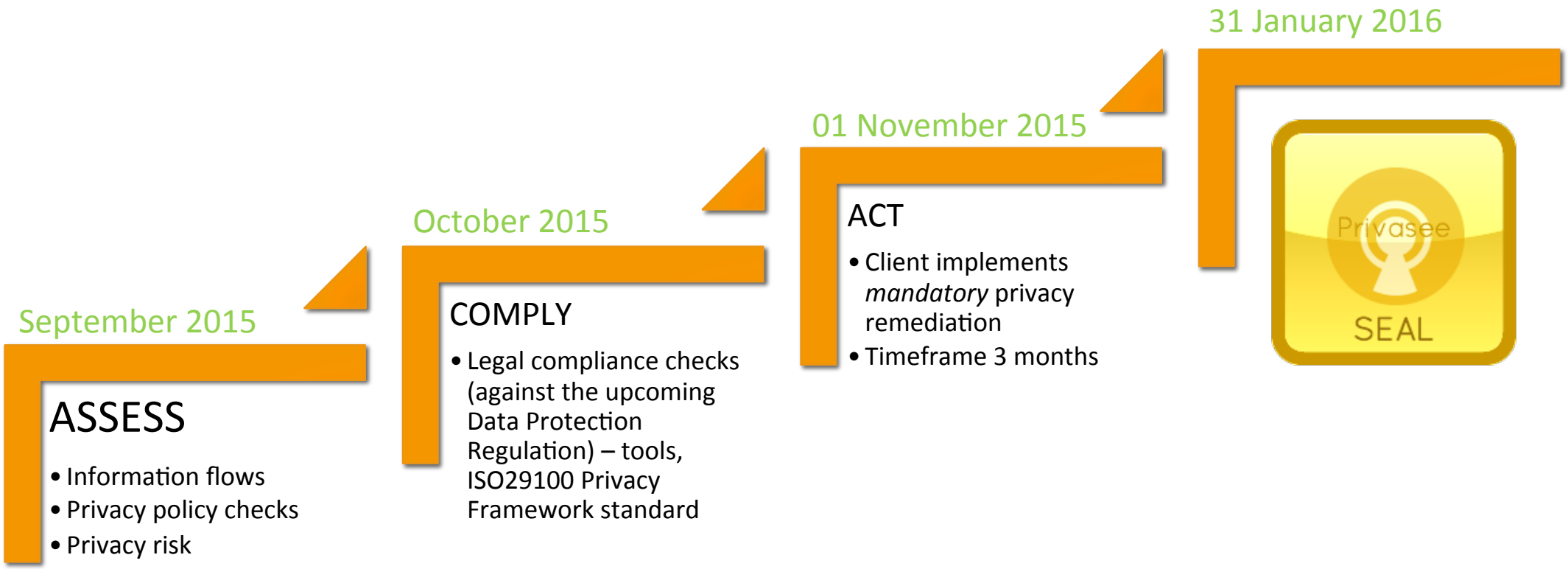
Threshold Assessment

1. A mailbox service in the cloud has been made available for the global market which collects personal data purely in order for it to operate;
2. The type of personal data collected makes this a ‘low privacy risk’ category;
3. The new Data Protection Regulation places new privacy demands beyond what is expected today.

Scope

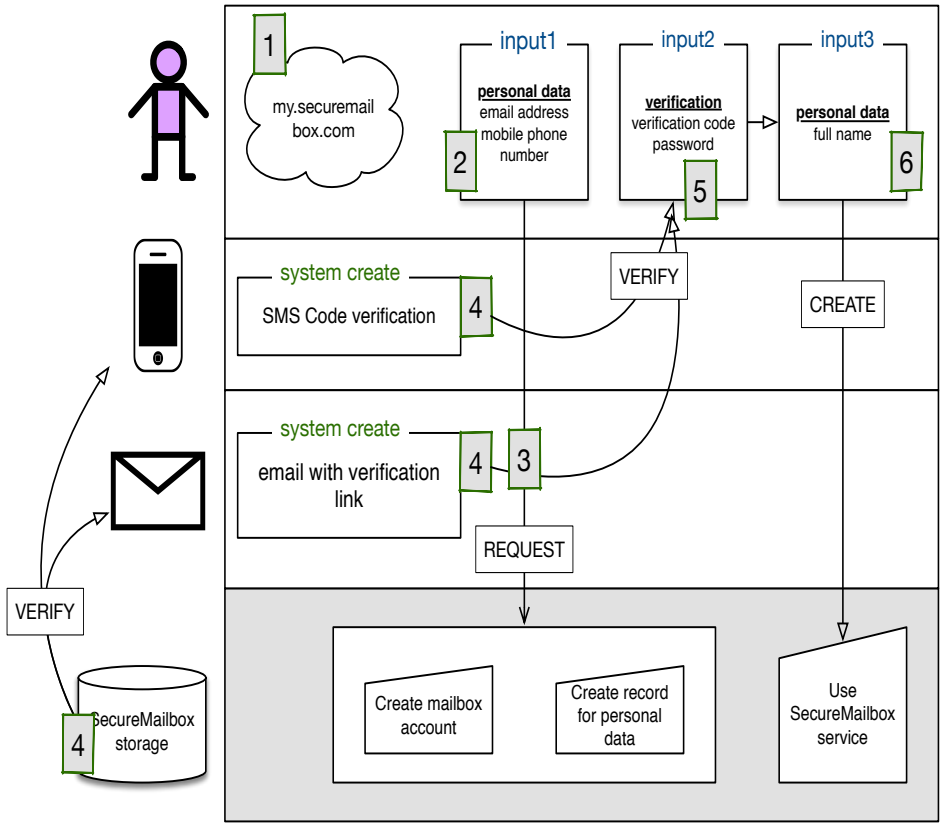
Types of data	Types of privacy	Legislation
email contents, personal data and communications' meta-data	Information privacy, communication privacy	The upcoming Data Protection Regulation (GDPR)

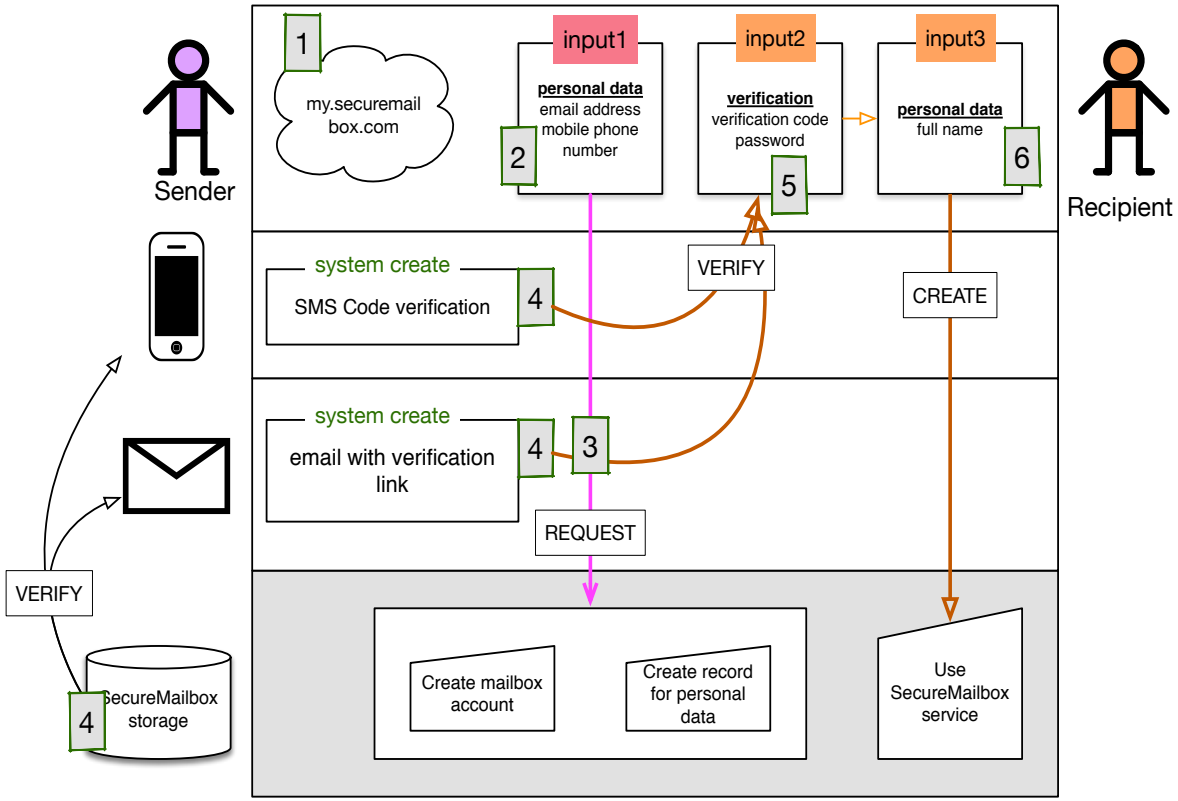
SecureMailbox Privasee SEAL Journey



SecureMailbox Personal Data Flows

There are two data-flows:





A) User creates SecureMailbox

B) Requestor initiates creation of SecureMailbox for Recipient of e-mail message

Privacy Policy Check

	Privacy Principles of ISO/IEC 29100		SecureMailbox
1	Consent and choice	✔	Explicit' consent on service acceptance & 'unambiguous' consent on policy updates
2	Purpose legitimacy and specification	✔	Personal data is collected for a specific purpose which is just enough to enable the service to function, no more.
3	Collection limitation	✔	The only personal data collected is within the boundaries of the purpose for collection.
4	Data minimisation	✔	Personal data collected is not used outside of the bare essentials of the service.
5	Use, retention and disclosure limitation	✔	Personal data collected is stored for only as long as is necessary for the service to function. Personal data collected on non-validated mailbox accounts is kept for 8 weeks. If the mailbox is not validated in this time, it is deleted.
6	Accuracy and quality	✔	Users of the service have unhindered access to view and modify personal data stored on them within the service.
7	Openness, transparency and notice	✔	No comment
8	Individual participation and access	✔	Self-service
9	Accountability	N/A	To be reassessed once GDPR is implemented in 2018.
10	Information security	✔	Evidence of sufficient security measures are implemented.
11	Privacy compliance	✔	Compliance with ISO29100 aligned with award of 'Privasee SEAL'

Privacy risks

SecureMailbox is only collecting personal data that is absolutely necessary for the service to operate. In this way they have minimized privacy risks. Listed below are privacy risks accepted but minimized with some mitigations provided alongside the identified risk.

#	Problematic data action	SecureMailbox action	GDPR reference	ISO29100 mapping
4	User telephone number (personal data) is visible to all contacts by default on old accounts.	Notify all existing users that they have the option to change this option.	Art (30)(2)	5. Use, retention and disclosure limitation
5	An invited user did not consent to the use of their personal data to create an account	It is email address and telephone number, that is deleted after 8 weeks if the account is not activated.	Art 6(a)	1. Consent and choice
6	User sends personal data or/and sensitive data in the email subject header, and the user is unaware that it is not encrypted when in transit, it is exposed for example in the notification message if switched on.	User is informed in the Privacy Notice.	Art (30)(2)	7. Openness, transparency and notice

Legal Compliance GDPR

SecureMailbox is fully compliant with the GDPR as far is can be assessed January 2016.

- Detailed assessment available in supporting report;
- Certificate issued separately.

In 2018 a reassessment against the finalized GDPR implementation once the infrastructure for the Data Protection Commission is implemented will be done.