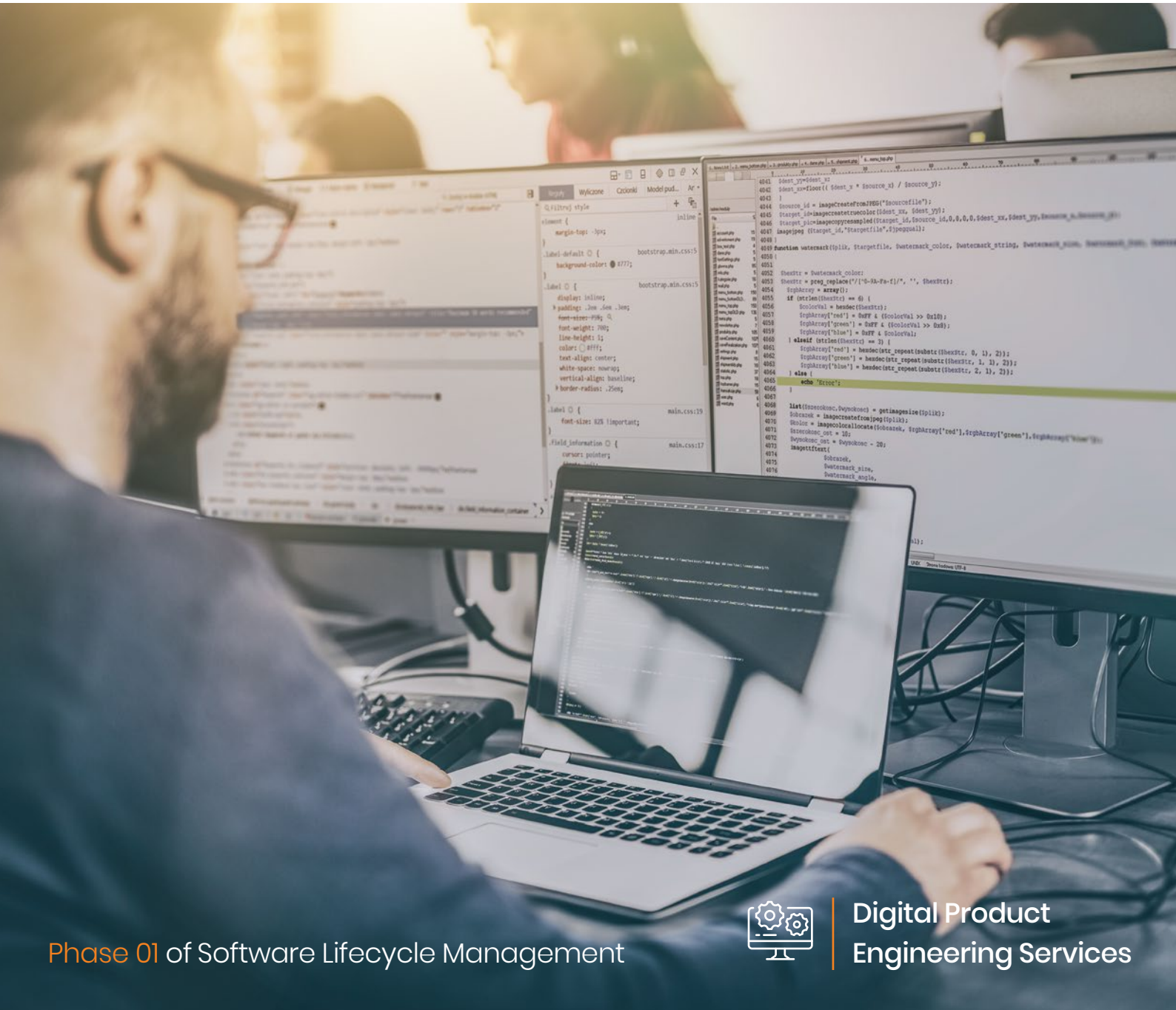
ACL Digital
an ALTEN group company

Requirement Lifecycle Management

This whitepaper provides a detailed account of cybersecurity and data protection requirement guidelines for the first phase of the Software Lifecycle Management



Phase 01 of Software Lifecycle Management

Digital Product Engineering Services

Table of contents

Introduction

The Business Analysis Body of Knowledge (BABOK) published by the International Institute of Business Analytics (IIBA) describes the Requirement Lifecycle Management as one of the key knowledge areas that describe the tasks that business analysts perform in order to manage and maintain requirements and design information from inception to retirement. The purpose of Requirements Lifecycle Management is to ensure that the requirements from all the stakeholders (direct, indirect, external and internal) are adequately assessed, captured, approved and centrally managed.

While modelling the other product requirements, it becomes imperative to capture all aspects of cybersecurity and data privacy as part of these requirements. It is for this purpose, that the various cybersecurity processes and standards are consolidated and added as separate lists of epics which are further elaborated into user stories for easy implementation.

> **"At ACL Digital we have a consolidated set of user stories in Jira covering NIST 800-53, SSDF or CIS Critical Security controls, HITRUST CSF, COBIT, ISO/IEC 27000 family, OWASP Top 10, CWE, HIPAA, PCI, SOC, GDPR, CCPA, CLOUD Act, Security considerations for Cloud computing, ISACA. You can extract your own required user stories from this comprehensive list by selecting sections that apply to your product and combine them with your product requirements. This will provide an initial jumpstart of 25% to your product development lifecycle!"**

There are few key aspects that one must carefully consider when dealing with cybersecurity requirements around identity and access management. NIST 800-53 is one of the most robust and prescriptive frameworks, with 18 control families and over 900 controls. The NIST Cyber Security Framework (CSF) is a subset of NIST 800-53, and is scalable and aligns with industry best practices for cybersecurity, making it an attractive option for commercial entities, especially those that are just starting to implement cybersecurity policies and controls.

Secure Identity and Access Management

The National Institute of Standards and Technology (NIST) 800-63-3 provides a four volume requirements set describing requirements for secure identity and access management.

1 **SP 800-63 Digital Identity Guidelines**

This provides the risk assessment methodology and an overview of general identity frameworks, using authenticators, credentials, and assertions together in a digital system, and a risk-based process of selecting assurance levels.

2 **SP 800-63A Enrollment and Identity Proofing**

This addresses how applicants can prove their identities and become enrolled as valid subjects within an identity system. It provides requirements for processes by which applicants can both proof and enroll at one of three different levels of risk mitigation in both remote and physically-present scenarios.

3 **SP 800-63B Authentication and Lifecycle Management**

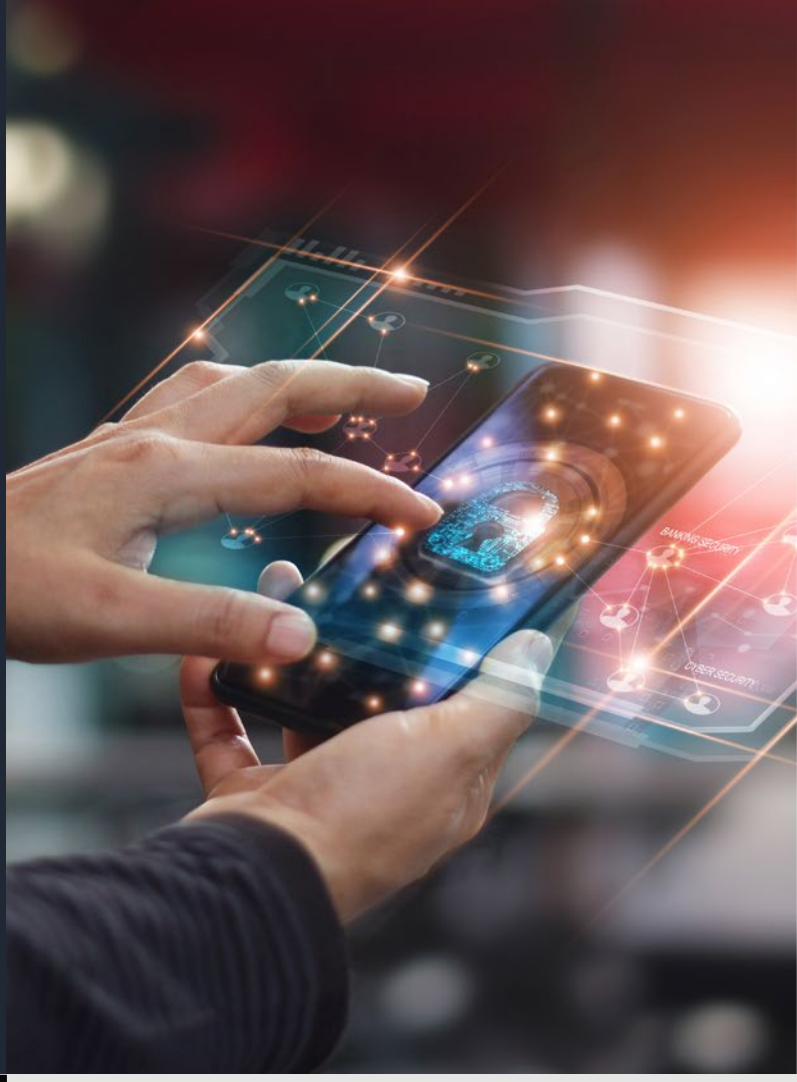
This addresses how an individual can securely authenticate to a Credential Service Provider to access a digital service or set of digital services. This volume also describes the process of binding an authenticator to an identity.

4 **SP 800-63C Federation and Assertions**

This provides requirements on the use of federated identity architectures and assertions to convey the results of authentication processes and relevant identity information to an agency application. Further, this volume offers privacy-enhancing computation techniques (PEC) to share information about a valid, authenticated subject, and describes methods that allow for strong multi-factor authentication (MFA) while the subject remains pseudonymous to the digital service.

Secure logging, audit and exception management

All applications need information to be logged in the form of user actions (audit trail), exception messages or logging information for debugging and / trouble-shooting purposes. The industry best practice is to mask all personally identifiable information (PII) that is being logged using any of these forms.



Privacy enhancing computation requirements

During the requirement elicitation process, it is highly recommended to identify and consolidate all personally identifiable information (PII) that are required to be processed as part of the application.

Privacy-enhancing computation aims at leveraging a group of various technologies to enable the highest level of data protection for PII data.

Compliance with data protection regulation requirements

The General Data Protection Regulation (GDPR) in Europe enforces stringent requirements for protecting personally identifiable information (PII data). It emphasizes on the need to provide a legal basis for collecting such personal data, typically in the form of consents. The data subject (whose personal data is being collected) has special rights which can be exercised in order to protect the data being collected. Corporations violating these rights are subject to heavy penalties. Therefore, it is recommended to include the following requirements into your Requirements Lifecycle Management phase.

The entity that captures the personal data from the data subject is called “controller”. The entity that processes the personal data either directly or on behalf of the controller is called “processor”.

Per GDPR article 30, an individual record needs to be maintained for each processing activity. This inventory of records is maintained as “record of processing activities” (ROPA).

There are eight fundamental data subject rights that need to be fulfilled through adequate technical requirements:

1. Right to information
2. Right to access
3. Right to rectification
4. Right to withdraw consent
5. Right to object
6. Right to object to automated processing
7. Right to be forgotten
8. Right to data portability

Data Subject Rights

1

Right to information

This right provides the data subject with the ability to ask a company for information about what personal data is being processed.

This requirement is fulfilled by providing a 'Privacy policy' document that informs the data subject about all processing activities and how is the personal data stored, purpose for processing, which data fields are processed, for how long is it processed, and so on. This document is provided as a link during user registration and the user's agreement consent needs to be captured against a timestamp. Every time this policy changes, the document link needs to be refreshed and the latest document version needs to be made available to the user.

2

Right to access

This right provides the data subject with the ability to get access to his or her personal data that is being processed.

This requirement is fulfilled by providing a user profile page or account details page that would allow the end user to maintain their own personal data record. They will always have all privileges to modify their personal data without any restrictions.

3

Right to rectification

This right provides the data subject with the ability to ask for modifications to their personal data in case the data subject believes that the data controller / processor is in possession of inaccurate data.

This requirement is fulfilled by providing a user profile page or account details page that would allow the end user to maintain their own personal data record. They will always have all privileges to request for modifying their personal data through any electronic medium (e.g. email, profile page, etc.)

Data Subject Rights

4

Right to withdraw consent

This right provides the data subject with the ability to withdraw a previously given consent for processing of their personal data for a purpose.

This requirement is fulfilled by providing a consent management page where the data subjects can manage their consents.

5

Right to object

This right provides the data subject with the ability to object to the processing of their personal data.

This requirement is fulfilled by providing an escalation process facilitated by the data controller or by providing an email address that captures such objections and concludes them by providing an effective follow-up cycle.

6

Right to object to automated processing

This right provides the data subject with the ability to object to a decision based on automated processing.

This requirement is fulfilled by providing an escalation process facilitated by the data controller or by providing an email address that captures such objections and concludes them by providing an effective follow-up cycle.

Data Subject Rights

7

Right to be forgotten

Also known as right to erasure, this right provides the data subject with the ability to ask for the deletion of their data.

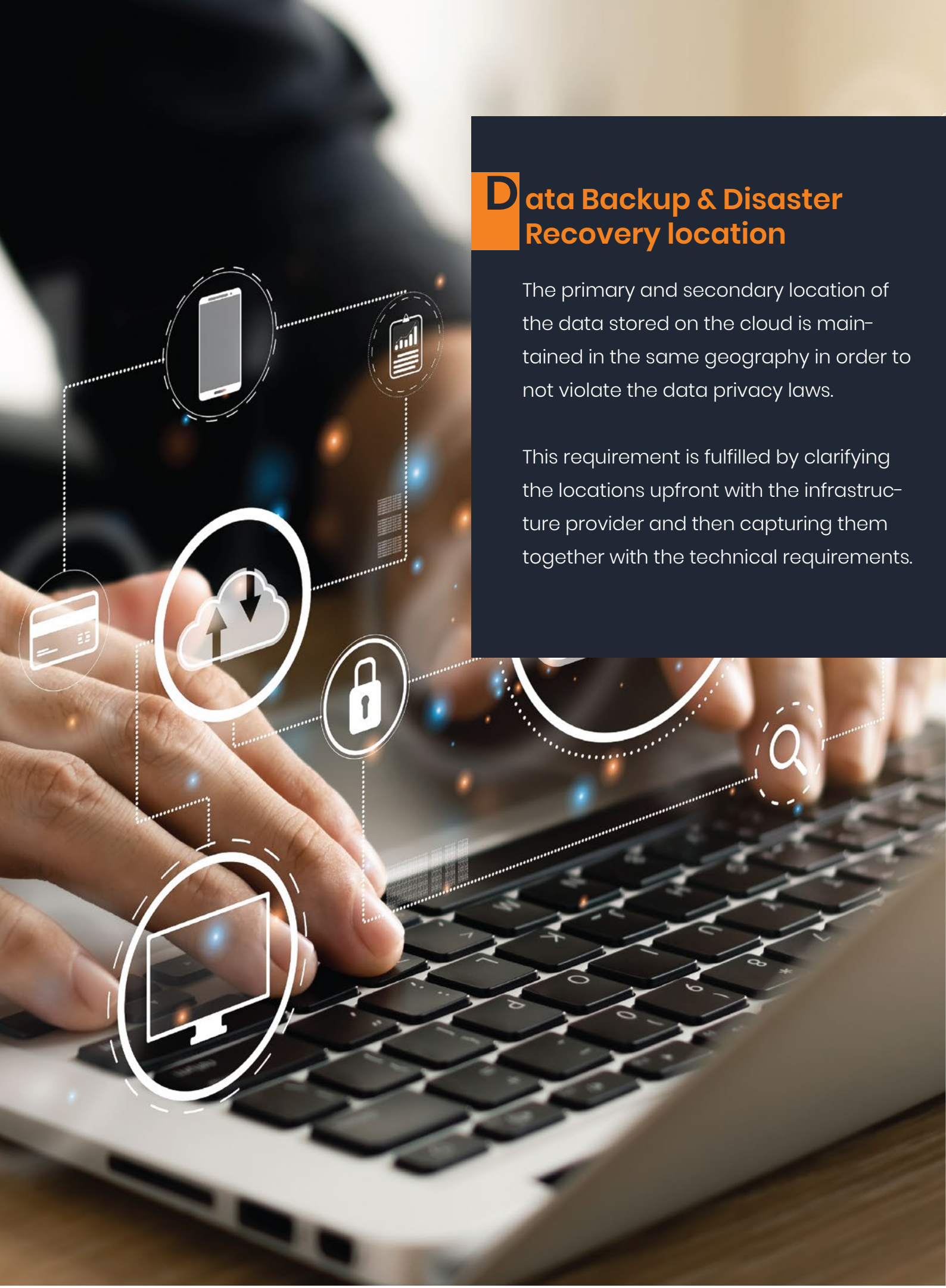
This requirement is fulfilled by providing a deletion concept explaining how the personal data would be completely removed from the software application. This includes retention period on the cloud before being permanently removed, mandatory retention periods legally implied by the local law of the land (e.g. invoices need to be legally retained for x years). When it is not possible for removing PII data permanently from all IT systems internally, the best practice is to anonymize such data.

8

Right to data portability

This allows individuals to obtain their own personal data that they have previously provided to the organization in a structured, commonly used, and machine-readable format.

This requirement is fulfilled by providing an escalation process facilitated by the data controller or by providing an email address that captures such objections and concludes them by providing an effective follow-up cycle.



Data Backup & Disaster Recovery location

The primary and secondary location of the data stored on the cloud is maintained in the same geography in order to not violate the data privacy laws.

This requirement is fulfilled by clarifying the locations upfront with the infrastructure provider and then capturing them together with the technical requirements.

References

- International Institute of Business Analysis: https://www.iiba.org/knowledgehub/business-analysis-body-of-knowledge-babok-guide
- Open Web Application Security Project® (OWASP) Top 10: https://owasp.org/Top10/A00_2021_How_to_use_the_OWASP_Top_10_as_a_standard/
- General Data Protection Regulation, Europe: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
- Privacy enhancing technologies: https://en.wikipedia.org/wiki/Privacy-enhancing_technologies
- NITS Cybersecurity Framework: https://www.nist.gov/cyberframework/online-learning/components-framework
- HITRUST CSF Framework: https://hitrustalliance.net/product-tool/hitrust-csf/