Digital Sovereignty

Security and privacy

EXAM fall 2025

Name	Initials	student number
Alexander Nygaard Thomsen	AT	201911329
Lecturer: Christian Damsgaard Jensen		

Due date: 11/12/2025

Contents

1 Executive Summary

The purpose of this report is the examine, expand and define the organizations current dependancy on non-EU technology, evaluate the key risks associated with this direction, analyse and propose EU alternatives. The goal is to identify and map a road to digital Sovereignty.

The current political climate is quite inhospitable and it has become apparent that world leaders make drastic, snap decisions that brings large implication to the technological landscape, where big tech can be leveraged as political thus inherently changing the risk of reliance on such servies. Thus companies, with suchs reliances, risks getting caught in the crossfire.

Services where there is a heavy reliance, from companies such a *Microsoft*, which hosts Azure Active directory (AD), used for identity management and *SharePoint* and *OneDrive*, which Lifeline Health Technologies(LHT) uses as a file sharing service, could suddenly become unavailable.

A loss of this service, which would be tantamount to loss of many years of technological IPs and achievements which could lead to unquantifiable damage to the company. Thus, in this inclimate weather, a EU alternative for these servises, is quintessential.

The main findings of this report is an overreliance on

- Microsoft Azure Services, where cloud hosting is indeterminate and jurisdictional expose is somewhat vague. Thus EU laws may be hard to apply
- process and regulatory mismatches - Data is easily given up to 3rd party cloud services without regard for compliance (EU MDR)
- A thorough documentation is needed of other cloud solutions, specifically regarding SaaS tools
- main risks

Examples for some EU-alternatives :

- Univention - German based software for identity & access management. A self hosted AD, requiring a virtual machine. Can then handle all authentication, along with other features such as single sign-on(SSO) and multifactor authentication (MFA)
- Scaleway - A cloud hosting service, to host VM's for infrastructre purposes.

Thus Univention can be hosted by Scaleway, thus removing the dependancy on a Microsoft service.
In addition, the company's productivity suite, can be replaced by libre-office

1.1 overall conclusion

2 Introduction

This report addresses the current and ongoing challenges that is present within Lifeline Health Technologies ApS due to the merger between Mediscan ApS, an established manufacturor of ultrasound electronics equipment for the health industry. And HealthSync Mobile ApS (HSM), a younger, digital health oriented company. The two former companies originates from two different times, with differing missions and complex implementatitons.

The complexity created by thtis merger and associated difficulties, due to differing it-landscapes, has prompted the executive team, to commission this report to highlight, identify and analyse the requirements and dependencies, related to digital Sovereignty with a focus on non-EU providers. The purpose of this report therefore becomes to identify risks within the newly formed, yet disjointed, It invironment which LHT has inherited, with its included assets, and how dependencies has could cause problems regarding regulatory compliance, operation stability and long-term autonomy from non-EU actors.

The scope of this report covers the broader themes of digital Sovereignty, including identity and access management, data-storage, infrastructre and process mismatches, aswell as the risk associated with a futrure migration along with a focus on jurisdictional factors that arises when handling sensitive data or other regulated information.

The overall structure of this report is, an overview of the current technology and service landscape of LHT, and a accompanying dependancy analysis. These two tie into the risk assessment of the current status. This is followed by an evaluation of possible EU-alternatives to implemented services and comparison of the current implementatitoon. Lastly a recommended migration Strategy is proposed.

3 Current Technology and Service Landscape

As a result of the merger between Mediscan Aps and HealthSync Mobile Aps, the it environment, inherited to LHT, is comprised to two very different digital landscapes. These difference goes beyond mere technocal platforms, such as tool chosen for various tasks, but also divering filosophies. This leaves LHT to operation in a Hybrid environment, where some parts of the company use incompatible identity systems, inconsistent governance practices and service providers that might not be a perfect fit for EU regulations.

3.1 Mediscan technology landscape

Mediscan originates from traditional engineering practies, around product development, production, calibration and quality asurance. These include

- On-prem EU-local infrastructre, there the whole it system is segmented into various sub networks, for engineering, manufacturing and servers.
- Local AD controllers, running on older operating systems, with weak overall governance
- Weak network security regarding hardware, older switches with no updates
- No MFA and relying on password update rotations

The infrastructre inherited from Mediscan, shows strong prefence to local storage and authentication along with a typical product first approach, where cynersecurity is seen as a hinderance.

3.2 HealthSync Mobile's technology landscape

HSM oprates a rather modern techonology environment, based in the new cloud computing era. With a heavy reliance on popular service providers such as the Microsoft Azure suite, Google cloud and other Saas products. These include:

- An extensize implementation of Azure services such as: AD, kubernetes, Cosmos DB, PostgreSQL, Key Vault, Api management, blob storage and monitor + application insights.
- Heavy reliance on CI/CD pipelines and API updates, from non-EU cloud hosted services.
- JSON/WIRE-formatted data.
- Enforced MFA, and OAtuh2 + OpenID for access to apps

HSM's modern Technology stack, which histroically has granted them the capability for rapid expansion and growth comes at the cost of strong ties to non-EU governed cloud services. Which could become subject to outside EU regulation.

3.3 The hybrid environment post merger

The post-merger leaves LHT with a partially integrated and partially improved hybrid network, currently consisting of:

- The legacy on-prem VLAN of Mediscan's solution for manufacturing and engineering
- HSM's Azure environment and dependencies
- Site-to-site VPN between the two company environments

Inconsistent and overlapping infrastructures creates uncertain flow between different parts of the company. This poses unknown and unmitigated risks, which could be leveraged as attack vectors and entry points.

3.4 Identity and Access management

An important integration issue is the overlapping domains, which results in some users need separate accounts to access multiple services. This leads to multiple services for the same purpose. This also introduces conflicting policies.

- Some users having multiple accounts, both on-prem and cloud.
- Azure AD policy, excludes the use of legacy hardware primarily found in Mediscan
- Inconsistent access rollout to internal file services such as Sharepoint.

Unnecessarily complicated access controls, which would require significant changes to the operation of the company infrastructre.

4 Dependency Analysis

4.1 Purpose

4.2 Dependency mapping

4.3 Current providers and dependency severity