IMPACT Privacy and Security Assessment

The Lebanese Ministry of Public Health (MoPH) and the Central Inspection partnered with donors to invest in the Inter-Ministerial and Municipal Platform for Assessment, Coordination and Tracking (IMPACT) to better respond to the pandemic. IMPACT has been handling and managing COVID-related services online, in partnership with MoPH: from mobility permits during lockdowns to vaccination registration. Most of the collected data is highly sensitive information about each individual, such as the full name, date of birth, place of residence, and ID number, as well as medical information. After a [follow up from SMEX](https://twitter.com/kataya_abd/status/1352612501201031169), IMPACT published its privacy policy pertaining to the COVAX platform and was last updated in February 2021.

SMEX has recently reviewed IMPACT’s privacy policy by comparing it to the European General Data Protection Regulation (GDPR) standards, since the data collected on IMPACT is housed in Germany, and Lebanon’s e-transaction law number 81/2018. We also provided a technical analysis of the platform and suggested some recommendations on its policies.

**Privacy Policy Assessment**

**Data Processing**

“We may use your personal data for research purposes,” states IMPACT’s privacy policy, without any indication to the type or entities conducting this “research.” According to the European Commission’s [**GDPR guidelines**](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227) and the [Lebanese e-transaction law number 81/2018](https://smex.org/wp-content/uploads/2018/10/E-transaction-law-Lebanon-Official-Gazette-English.pdf), the phrase above is not sufficiently clear as to the purposes of processing. This goes against article 87 of the e-transaction law, which states that: “Personal data shall be collected faithfully and for legitimate, specific and explicit purposes.” Similarly, it does not comply with GDPR guidelines as it is not very concise nor transparent.

**Data Retention**

In the subsection titled “Retention of Data,” the privacy policy states that: “The data is hosted on a server within Central Inspection. The data is also backed up on a server in Germany, managed by staff within Central Inspection.” This section also raises privacy concerns since the Lebanese law 81/2018 in its article 88 subsection 5 clearly states that the persons from whom the personal data are derived shall be informed of “persons to whom the data shall be sent.” In this case, it is unclear where the data is backed up in Germany and who has access to it. In addition, GDPR guidelines state that “the details regarding any transfer of personal data to a third country and the safeguards taken” should be clearly disclosed.

Furthermore, the privacy policy fails to mention for how long this data may be retained, it only states: “Retention of personal data shall be made **as long as necessary.**” This goes against both GDPR and article 90 of law 81/2018 which mentions that “retention of personal data shall not be legitimate except during the period specified in the declaration of processing or in the decision authorizing the same,” emphasizing that the retention period should be specific.

**Lodging a Complaint**

IMPACT’s privacy policy fails to provide the right to lodge a complaint with a supervisory authority, as stated in article 92 of law 81/2018: “Every natural person shall have the right to object, for legitimate reasons, before the data-processing officer to the collection and processing of his/her personal data.”  The GDPR guidelines also protect “the right to lodge a complaint with a supervisory authority.”

**Automated Decision-Making System/ License**

We also take note of the absence of an automated decision-making system as stated in article 86 of law 81 that stresses the need for “an automated processing” system, and the GDPR guidelines that emphasize the necessity of “the existence of an automated decision-making system, including information about how this system has been set up, the significance, and the consequences.”

It is also worth noting that the Lebanese law specifies in its article 98 the need for a “license or permit granted,” another point that the privacy policy failed to disclose.

While IMPACT’s privacy policy seeks to respect most of the criteria in the GDPR guideline and the Lebanese law, our findings reveal a number of privacy concerns, especially regarding IMPACT’s servers in Germany.

**Technical assessment**

After conducting a security analysis of IMPACT’s covax.moph.gov.lb and covid.pcm.gov.lb, we found no major security threats on the websites, but there remain some vulnerabilities that need to be addressed immediately.

# Covax.moph.gov.lb tech analysis

*Note: The same analysis applies to IMPACT’s* ***Covid.pcm.gov.lb*** *platform since the code and servers are the same, whereas the User Interface (UI) and the web services are different.*

**Servers in Germany**

IMPACT’s sub-platform for vaccine registration uses a German IP, with the main web-server located in Germany, at Leaseweb Deutschland GmbH Cloudstack Premium. The latter indicates that the hosting is based on Cloud technologies. Due to the nature of the data being collected at the Covax platform, **a clarification from MoPH and IMPACT is required** to understand where users’ data are stored. If it's stored in Germany, this issue must be addressed to ensure Lebanese citizens’ data is protected and stored privately.

**DoS attacks**

The Covax platform does not use [load balancing](https://en.wikipedia.org/wiki/Load_balancing_%28computing%29) (distribute a set of tasks on a set of resources), which might potentially endanger the web server to potential shutdown due to overload or potential [Denial-of-Service (DoS) attacks](https://en.wikipedia.org/wiki/Denial-of-service_attack).

**Not the best SSL encryption**

On another note, Covax does not use the best technology available for [Secure Sockets Layer (SSL)](https://en.wikipedia.org/wiki/Transport_Layer_Security) encryption, a protocol that ensures the security of communications over a computer network. SSL on Covax supports older versions of Transport Layer Security (TLS), TLS1.2, TLS1.0 and TLS1.1, which indicates that a potential TLS downgrade attack is possible.

The TLS protocol is used to encrypt communication between users and the servers, who are in this case the Lebanese citizens and the Covax platform. The latest TLS protocol is used only if the client (Chrome/Android/Iphone etc.) and the server support it. If both entities support a secure, not a vulnerable TLS protocol version in the communication, then it’s impossible to execute a [man-in-the-middle attack (MITM)](https://ar.wikipedia.org/wiki/%D9%87%D8%AC%D9%88%D9%85_%D8%A7%D9%84%D9%88%D8%B3%D9%8A%D8%B7), when the attacker secretly compromises the communications between two parties (mainly server and client devices). The [TLS downgrade attack](https://en.wikipedia.org/wiki/Downgrade_attack) can trick the client device to use an older TLS vulnerable version for encrypting the information in transit. The attacker then tries to intercept the information and exploit flaws in the older protocol version or weak cryptographic algorithms.

**Covax should address this issue by ending support to vulnerable TLS versions including TLS1.0 and TLS1.1**

**Potential Clickjacking attacks**

We discovered that the Covax platform might be a target for [Clickjacking attacks](https://en.wikipedia.org/wiki/Clickjacking) because of the lack of security parameters on the server side. Clickjacking is an interface-based attack (the webview on the user’s side) in which a user is tricked into clicking on actionable content on a hidden website by clicking on some other content in a malicious website.

The risk is low but clickjacking potential attack means facilitation for phishing attacks.

**No Firewall**

IMPACT’s Covax platform has no firewall on the server side. From our technical analysis, we couldn’t identify the presence of a firewall on the Covax web server, which indicates a lack of basic security on the server and the inability to identify potential threats to Lebanese citizens' privacy and data.

**Shared Web Service**

Lastly, Covax platform also provides a web service based on Jetty service. This service is probably accessible to other governmental entities and can be used to retrieve information or access the data available on the Covax platform. We identified the version of Jetty to be Jetty 9.4.36.v20210114. It’s severity is medium but could potentially lead to an important impact on the Covax platform. When Jetty handles a request containing multiple Accept headers (specially cracked) with a large number of specific parameters, the server may enter a Denial of Service (DoS) state due to high CPU used processing those quality values, resulting in minutes of CPU time exhausted processing those quality values.

**Conclusion**

IMPACT's online platforms have played a huge role in facilitating a swift response to the pandemic, yet some risks to privacy and security have not been properly resolved or addressed. For instance, its privacy policy fails to disclose some critical information about the retention and processing of personal data. In addition, our technical analysis has revealed some vulnerabilities that might compromise data collected on the platform. We ask IMPACT to deploy the latest and most advanced security measures when handling people's personal records and medical background; be more transparent regarding the servers and publish a transparency report explaining why the server is located in Germany, how users’ data are being stored and processed, and who can access and process this data.

We are ready to help with new apps and websites looking to fortify their privacy and security, and we will – in partnership with [Friedrich Naumann Foundation](https://www.freiheit.org/lebanon-and-syria) (FNF) Lebanon and Syria – expand our work on serving as a watchdog over citizens’ digital data on Lebanon’s government platforms.