Clarifying the Treatment of Children's Data in IMTLazarus

Introduction

This document aims to clarify for families, primarily in a question-and-answer format, how their children's data is handled in IMTLazarus.

Families want to be sure that the school does not access personal information about students. So, How does IMTLazarus protect student data?

IMTLazarus sets up a school calendar and timetable in which NOBODY has access to management and information of the device outside of school hours. In IMTLazarus, we maintain a strict separation between the educational and family spheres.

Does the installation of the app on personal devices have consequences?

We allow for safe browsing on the internet without significantly impacting device performance. Your device will not be significantly affected.

Can I disable the app at home?

To ensure that children are safe both in and out of school, we must protect the whole community and avoid creating individual exceptions by disabling the application.

We are concerned about the possible security vulnerability that the IMTLazarus application could generate on the devices.

Far from violating security, the IMTLazarus application ensures this strengthening a sense of protection. This protection helps prevent exposure to inappropriate content that could harm children's health and development. Controlling access to content is essential to ensure it is suitable for their age.

Where are the servers used to store our students' data physically located?

The IMTLazarus infrastructure is based on OVHcloud, a French company that is the leader in Europe in this sector. Our data centers are located in France (Strasbourg and Gravelines) complying with the European legislation on data processing (GDPR).

Which service providers are employed and what certifications or security measures are in place to ensure compliance with data protection legislation?

The IMTLazarus platform is provided as a cloud service through which communications with agents implemented in different device technologies are centralized. Communications are made through encrypted connections.

As mentioned we use a single OVHcloud provider. The level of access to the platform is regulated by the profile of the identified user.

It is important to note that the company OVHcloud has ISO/IEC 27001, 27017 and 27018 certifications and reports and also offers anti-DDoS protection as standard. Additionally, IMTLazarus has an automated backup system for high availability.