- **The minimum version required of the following web browsers in order for your software to work properly:**
  - **Safari;**
  - **Firefox;**
  - **Chrome;**

https://knowledge.kaltura.com/help/kaltura-player-supported-browsers-devices

- **The URL of the page of your site from where you can download the CSA STAR Self-Assessment report:**
  - **They want to see from where, in your official site, a user can access the self-assessment report, so you need to publish it somewhere visible and accessible in your public website and send me the URL to that page, you can also put the link to the self-assessment report directly in the footer of your website or in a page regarding your security policies**

We have completed the CAIQ and it is available here: https://corp.kaltura.com/wp-content/uploads/2020/06/Kaltura-Completed-CAIQ_v3.1-for-AGID.xlsx

- ~~**API authentication methods:**~~

~~I've already found it directly from your API documentation website~~

- **They need more info about your personal data protection policy, more specifically they need:**
  - **the methods in which the data are stored and archived;**

Customer data will be physically stored in AWS data centres and encrypted at rest (https://aws.amazon.com/compliance/data-center/controls/). In addition, Kaltura platform uses a multi-tenancy environment and all customer content and metadata stored on the Kaltura platform is logically segregated from the content of other customers by assigning each item to an unique partner ID associated with the customer account in the Kaltura SaaS platform database. Every interaction with the platform use a Kaltura Session token which includes a customer id. The session prevents the application from accessing any other customer data.
Kaltura's data centres utilize a multi-tenant, shared infrastructure. There are both physical and logical layers that separate customer content. Access to the Kaltura business logic, and the content and data maintained in the system can only be achieved through the Kaltura API. The Kaltura API includes a security mechanism to ensure that only authorized users and systems can perform any actions through the API.
The Kaltura Session (KS) is the most fundamental level of Kaltura's security implementation. The KS is an authentication token that must be supplied as a parameter to all Kaltura API calls.

  - **the security measures in place in the event of unauthorized access;**

A Security Incident may be handled in a variety of ways based on its source and potential damage. However, the general process of responding to such an incident will include the following steps:

Preliminary analysis, data gathering and documentation – The IT Manager will gather the information from internal sources (users, members of the System Team, etc.) as well as from external sources (Internet, publicly published information, external specialists, advisors, etc.). All relevant information should be gathered and stored.

Immediate response – In any case in which the incident is not over, the IT Manager and the CISO shall take measures to resolve the incident and prevent further damage as quickly as possible.

Preservation of evidence - If the source of the event is a result of an employee's policy violation or if the incident requires legal action, all data and evidence must be retained and protected. Maintaining the integrity and reliability of the evidence is crucial for cases in which legal actions may take place. The Senior Director of Legal Affairs (or comparable senior member of the Legal Department) shall advise regarding the preservation of evidence.

Involvement of a response team – Security incidents that cause significant damage to core business services will be managed by the CISO and will be reported immediately to a response team, whose members will include: Senior VP of Operations; CISO; VP of Customer Success; and the IT Manager. In the event that there is suspicion of a data breach, the response team will also include the CEO, CTO, CMO, and Senior Director of Legal Affairs (or comparable senior member of the Legal Department).

Analysis – The CISO shall analyze the information gathered and identify the following elements:

- Source of the event.
- Systems involved in the incident (whether damaged or could be damaged by the incident).
- Potential impact of the incident on the systems, their integrity, confidentiality and availability.
- Current status of the incident (over, continuing, etc.).

Communications plan – The response team will devise and implement a communications plan for the incident. Relevant facts will be communicated in a timely manner as necessary to affected customers, internal stakeholders, and the public.

Learning from mistakes – After the event is over, the IT Manager and CISO shall study the event in order to identify and understand the breaches, vulnerabilities and malfunctions which enabled the incident to occur and define the measures which must be taken in order to prevent a reoccurrence of the event.

Concluding report – The CISO shall issue a report which will include the following elements:

- System manager details.
- Time and date of the event.
- Specific description of the event.
- Description of the actions that were taken (if applicable).
- Recommended actions

    - **the presence of tools to monitor data security levels;**

As a cloud-based SaaS offering, the majority of system and infrastructure monitoring is handled by Kaltura's operations staff. Kaltura’s IT Team uses a variety of state-of-the-art internal and external intrusion detection, intrusion prevention, and network monitoring tools to detect and prevent unauthorized activity throughout the company's computing systems and network components (Production servers’ operating systems, network servers, applications, etc.).

Kaltura has security and hardening standards for network devices (baseline configuration, patching, passwords, access control), and regular review and monitoring of network devices for continued compliance to security requirements according to ISO27001 standards.
Kaltura leverages industry standard tools and independent industry standard 3rd party services for vulnerability testing, hardening, and monitoring. This includes:
- Weekly vulnerability scans by McAfee Secure
- Annual Penetration testing by 3rd party vendor
- Annual Code review by 3rd party vendor
- Annual Risk Assessment
- Customer's Penetration Testing and audits

The Information Head of Security initiates risk surveys and penetration tests for different systems in the company. High-risk systems are tested at least once every year, or following major system changes. Other systems are tested at different time periods according to their sensitivity, and at the Information Head of Security's discretion.

- **the timing and methods by which any data breaches are managed and communicated;**

Kaltura maintains a documented Incident Response Policy. Affected customers are notified within 24 hours of discovery. Outreach will include the nature of the incident, name and details of Kaltura's DPO, likely consequences of the incident, and remediation plan to address the incident.

- **the ways in which access to data can be restricted;**

The Kaltura platform was built with security being an essential component of any new service. The primary security mechanisms for protecting content and data are implemented at the API layer where strict access controls can be applied and configured according to each customer's requirements.

Kaltura's API authenticates every call (request) made to the Kaltura API with an authentication key, the Kaltura Session (KS), identifying the account on which the action to be carried, the authenticated user and its role. The KS expiry can be set at session initiation to range from 1 second to 10 years. The KS can also be limited by the number of API calls it authenticated. The KS is generated based on a secure shared secret, which is not transmitted over the wire. For more information, see here: *http://knowledge.kaltura.com/kalturas-api-authentication-and-security*.

- **Availability of some kind of insurance coverage in relation to the privacy risk.**

Kaltura maintains Cyber Liability Coverage for this purpose.