Flare - Security Addendum

Version 1.0 - Effective on 2024-07-01.

This Security Addendum describes the technical and organisational security measures implemented by Flare in providing the Services under the Terms of Service.

Flare will deploy technical and organizational measures as reasonably required to protect Customer Data, including Personal Data, taking into consideration the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risks to security and privacy. The security measures implemented by Flare include the following:

1. Policy Framework and Organisation

Flare maintains and communicates internally a formally documented security policy, including cybersecurity functions with clearly defined roles, responsibilities and processes, consistent with industry standards.

2. Human Resources Security

2.1 Flare conducts comprehensive background checks, including employment and criminal record verifications, on its employees, consultants, and other Representatives who may have access to Customer Data, before engaging them.

2.2 If any background check is not cleared or discloses that a Representative has misrepresented any information, Flare will not permit such a Representative to access Customer Data or systems processing Customer Data or perform any Services for Customer.

2.3 Flare provides initial and ongoing training and awareness on security and data protection requirements to all its Representatives who have access to Customer Data, commensurate with their level of responsibility for Customer Data.

2.4 Any Representative who may have access to Customer Data is bound by a confidentiality agreement.

3. Data Retention and Deletion

3.1 Customer Data is securely deleted from all electronic media when defective, sent for repair, no longer required or reused, or the media itself is securely destroyed.

3.2 Upon termination or expiry of the Terms of Service, but no later than 30 days thereafter unless approved by Customer, Flare securely destroys or deletes, and requires the same from its sub-processors, all Customer Data subject to the Terms of Service, including data on backup media and backup sites, unless strictly required by law to retain it.

3.3 Upon termination of expiry of the Terms of Service, this Addendum will continue to apply for as long as Customer Data is kept by Flare.

4. Access Control

4.1 All physical and logical accesses to Customer Data and systems processing Customer Data are granted on a “need-to-know” and “least privilege” basis.

4.2 Roles and responsibilities for anyone having access to Customer Data are defined in a manner that allows for appropriate segregation of duties to address conflicts of interest.

4.3 All user accounts are personal accounts and account credentials are not shared between users under any circumstances. Shared accounts are prohibited.

4.4 All administrator accounts, remote access accounts and all accesses to Customer Data use a multi-factor authentication mechanism (MFA).

4.5 All accesses to Customer Data are reviewed and certified on a regular basis by Flare management.

4.6 Account deactivation and deletion if performed promptly, including access to Flare facilities, immediately upon employment termination, reassignment, or the end of a contract.

4.7 Security logs are generated, reviewed, retained and available for a minimum of one year.

4.8 Flare will inform Customer promptly in the event access to Customer Data is sought by a third party, including law enforcement agencies, unless prohibited by law to do so, and shall follow Customer instructions concerning steps to be taken to protect Customer Data from disclosure.

5. Separation of Environments

5.1 Flare ensures appropriate logical or physical separation of Customer Data from data of other clients.

5.2 Flare provides separate technological environments for production and other activities (development, test, quality assurance, etc.) and clear segregation of duties for personnel accessing these environments.

5.3 Customer Data is not replicated or used in non-production environments, unless it is first anonymized, meaning that data can no longer be used to identify the Customer or an individual directly or indirectly.

6. Cryptography

6.1 All Customer Data is encrypted throughout its life cycle, at rest and in transit, using commercially available strong encryption technology. Flare follows industry-accepted sunsetting schedules for deprecated encryption standards.

6.2 Encryption key management and key usage is not performed by the same individual.

7. Physical Security

7.1 Customer Data and the systems processing Customer Data are located in secured locations.

7.2 Data centres used for the processing of Customer Data meet industry requirements for data centres, corresponding to the sensitivity of the data processed in terms of confidentiality, integrity, and availability.

8. Network Security

Adequate network security measures are implemented in our environments and those of our sub-processors, including:

- Next-Generation Firewalls
- Intrusion prevention and detection (IPS/IDS)
- Wireless (Wi-Fi) network security
- Virtual private networks (VPN) for external accesses
- Network segmentation
- Web, email, application, and database server security (Hardening)

- Terminal security, including desktops, laptops, and mobile devices (EPP/EDR)
- Data loss prevention (DLP)
- Malware detection (AV)
- Security information and event management (SIEM)

9. Vulnerabilities

9.1 Vulnerability scans are performed on a quarterly basis and penetration testing is performed on a yearly basis and upon significant changes on all systems and software processing Customer Data.

9.2 System and software vulnerabilities are addressed and security patches or new versions are made available to customer or applied to Flare systems and software in a timely fashion, but within 48 hours for critical vulnerabilities, within 2 weeks for high vulnerabilities, within 3 months for medium vulnerabilities and within a year for low vulnerabilities.

9.3 Systems processing Customer Data are protected with up-to-date anti-malware solutions to prevent, detect, and remove known malware.

10. Changes

10.1 A change management process is in place for all changes that may impact the Services.

10.2 System processing Customer Data may not be modified in a way that could materially impact functionality of the Services or confidentiality, integrity or availability of Customer Data without prior notice to Customer.

11. Incident Response and Data Breaches

11.1 Flare maintains an incident response plan to address detection, analysis, containment, eradication and recovery from incidents, along with application of lessons learned.

11.2 Flare will notify Customer promptly via email upon detection or suspicion of a Client Data breach, or upon any incident that requires the execution of a business continuity or disaster recovery plan.

11.3 Flare will not make or permit any statement, concerning Customer Data impacted by a data breach, to any third party, unless required by law to do so or if prior Customer approval is obtained.

12. Business Continuity and Disaster Recovery

Flare maintains and regularly tests, at a minimum on a yearly basis, business continuity and disaster recovery plans, for all locations used to provide the Services, to ensure continuity of the Services to Customer, in accordance with the service level objectives found in the Terms of Service.

13. Secure Development

13.1 Flare follows applicable secure coding best practices (OWASP guidelines) to ensure that all applications and systems that process Customer Data are securely developed.

13.2 Flare does not, under any circumstance, embed any mechanism within its applications or systems that process Customer Data to monitor or report user behaviour or send any Customer Data to a third party, unless it is absolutely required for the application or system to operate, in which case it is fully disclosed to Customer.

14. Data Localization

Data centre locations, where Customer Data is processed, for both primary and secondary sites, and sites where backups are kept, are located in AWS us-east-1 (N. Virginia) and AWS ca-central-1(Montréal) regions.

15. Compliance and Audits

15.1 Flare maintains a yearly SOC 2 Type II audit report, performed by an independent and reputable auditor, covering the security criteria, which can be made available to Customer upon request.

15.2 Upon request, Flare may provide to Customer any additional information that may be required to demonstrate compliance with the current Security Addendum.

16. Sub-processing

16.1 Flare uses sub-processors to perform certain activities in order to provide the Services.

16.2 Flare will not share Customer Data with any sub-processor unless the sub-processor is contractually bound to comply with this Security Addendum or equivalent.