Data Processing Agreement

Version Date: 1 October 2023

adyen

engineered
for ambition

Table of Contents

Data Processing Agreement

Effective as of 1 October 2023

This Data Processing Agreement ("**DPA**") is entered into between Adyen and Merchant (each a "Party" together the "Parties") and will form an integral part of the Merchant Agreement. In the event of any inconsistency arising between the provisions of this DPA and the Merchant Agreement, the provisions of this DPA shall prevail.

Any terms not defined in this DPA shall be as defined in the Merchant Agreement.

Article 1. Considering

Data Protection Laws require that any Processing of Personal Data by a Processor will be governed by an agreement between such Processor and Controller and otherwise, that the Parties conduct an assessment of their roles for any Processing; therefore, Parties wish to further define their data processing relationship in accordance with the agreements as set out in this DPA.

1.1 Definitions and Interpretations

In this DPA the terms "Controller", "Data Subject", "Personal Data", "Process", "Processor", "Pseudonymization" and "Supervisory Authority" will have the meanings ascribed to them under Data Protection Laws or, where not specifically defined, the meanings of analogous terms under Data Protection Laws.

The following words and phrases shall have the following meaning:

"**Acquiring Services**" means a payment service resulting in a transfer of funds to the Merchant through Adyen, which entails the authorizing, recording, clearing and settling of Transactions in accordance with the Scheme Rules.

"**Adyen Services**" as described in the Merchant Agreement and Services Description.

"**Data Protection Laws**" means any data protection law, where applicable to a party including the EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

"**Employee**" means any employee, agent contractor, work-for-hire or any other person working under the direct authority of a Party.

"**Instruction**" means the documented instruction from Controller to Processor to perform a specific action in accordance with the Merchant Agreement (including all Schedules thereto), which directly or indirectly entails the Processing of Personal Data.

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

"**Restricted Transfer**" means a transfer of Personal Data or an onward transfer of Personal Data (including between two establishments), in each case, where such transfer would be prohibited by Data Protection Laws in the absence of an appropriate data transfer safeguard.

"**Sub-Processor**" means any entity engaged by Processor to Process Personal Data on Processor's behalf.

Article 2. Roles and Applicable Terms

2.1

In respect of Adyen's Processing of any Personal Data for the Adyen Services in the capacity of a Processor, the terms of Annex 1 of this DPA shall apply to the extent Adyen is regarded as the Processor.

2.2

In respect of Adyen's Processing of any Personal Data in the capacity of a Controller, including for the provision of the Acquiring Services under the Merchant Agreement, in relation to Adyen's Processing of any Merchant business contact

information or "Know Your Customer" information as required under anti-money laundering and counter-terrorism financing laws and in relation to any additional new Adyen Services or features of the Adyen Services where Adyen takes on a Controller role, the terms of Annex 2 of this DPA shall apply. The processing of Personal Data for these purposes are governed by the Adyen Privacy Policy (available online on adyen.com or at any other successor website), as amended from time to time.

This DPA is agreed and entered into as set out below.

Annexes which form part of this DPA:

Annex 1: Controller to Processor Terms

Annex 2: Controller to Controller Terms

Annex 3 Specific Local Requirements

Annex 4: Personal Data Protection and Security Program

Annex 5: Description of Processing

Annex 6: Standard Contractual Clauses (Processor to Processor) – provided separately

Data Processing Agreement – Annex 1 – Controller to Processor Terms

Article 1. Scope of Processing and General Obligations

1.1

For the Processing of Personal Data under the Agreement where Merchant acts as a Controller and Adyen acts as a Processor, Parties agree to the terms of this DPA. Each Party undertakes to comply with its obligations under the Data Protection Laws and is solely responsible for compliance with the Data Protection Laws that apply to them.

1.2

Processor will Process Personal Data in a manner consistent with this DPA, the Instructions of Controller, and/or to the extent necessary to provide the Services to the Controller under the Agreement and in accordance with Applicable Laws. Annex 5 of this DPA contains a description of these Processing activities.

1.3

Controller decides which data categories will be sent to Processor. Controller (and its auditors) will have access to the Personal Data Processed by Processor through the Customer Area.

1.4

The Merchant Agreement and this DPA shall be seen as Instructions from Controller to Processor for the Processing of Personal Data. Controller is responsible for ensuring that the Instructions it provides to Processor to Process the Personal Data are in accordance with any Applicable Laws (including Data Protection Laws). In case of an infringement of such laws, Controller shall indemnify and hold Processor harmless for any claims or complaint from a Data Subject following therefrom. Processor shall notify Controller as soon as it believes an Instruction from Controller might be violating any Data Protection Laws. Any failure by Processor to notify Controller shall not affect Controller's responsibility and liability for its Instructions.

1.5

For the avoidance of doubt, Processor is not responsible for the Processing of Personal Data by third parties where such Personal Data is sent by Processor on the Instruction of Controller such as Scheme Owners and other Acquirers. The Processing done by those parties is not governed by this DPA.

Article 2. Data Subject

2.1

Processor has no direct relationship with the Data Subject and shall inform Data Subjects to contact Controller first. Processor shall notify Controller without undue delay, unless specifically prohibited by Applicable Laws and regulations, if Processor receives:

- any individual rights requests with respect to Personal Data Processed;
- any complaint relating to the Processing of Personal Data, including allegations that the Processing infringes on a Data Subject's rights under Data Protection Law; or
- any order, demand, warrant, or any other document purporting to compel the production of Personal Data under Applicable Law.

Processor shall not respond to any of the above unless expressly authorized to do so by the Controller or as obligated under Applicable Law or a court.

2.2

Processor shall reasonably cooperate with Controller and assist Controller with respect to any action taken relating to such request, complaint, order or other document as described under Clause 2.1. As far as reasonably possible and taking into account the nature of the Processing, the information available to Processor, industry practices and costs, Processor will implement appropriate technical and organizational measures to provide Controller with such cooperation and assistance. Where the required information can be retrieved by Controller itself from the systems of Processor through the Customer Area made available by Processor, Controller will retrieve such information itself from the systems of Processor.

Article 3. Data Location

3.1

Processor shall store Personal Data of Controller solely in data centers located in the EU, except on specific Instruction of Controller. Personal Data originated outside of the EU may also be Processed on local or regional servers. Controller understands and agrees that for the fulfilment of the Merchant Agreement, Personal Data may be accessed by Employees of Processor and/or Sub-Processor, which might be located outside of the EU. Parties shall ensure that appropriate measures under Data Protection Laws are in place. The Standard Contractual Clauses in Annex 6 safeguard the data transfer to Sub-Processors.

3.2

Processor (as "data exporter") and Sub-Processor(s) (as "data importer") with effect from the commencement of a Restricted Transfer hereby enter into the Processor to Processor Standard Contractual Clauses in respect of any transfer to Processor (or onward transfer) where such transfer would otherwise be prohibited by Data Protection Laws.

3.3

Where Personal Data is Processed in the United States or any other jurisdiction which does not offer an adequate level of protection to Data Subjects as equivalent to the protection in the European Union and/or the United Kingdom, in the event that a subpoena and/or disclosure request is received from a national organization (for example relating to national security purposes) which covers Personal Data relevant to, and/or which would involve disclosing Personal Data identifying, a Data Subject in the United Kingdom and/or European Union: the Processor shall, and shall procure that each Sub-Processor shall: (a) immediately notify the Controller (if and to the extent permissible by law); (b) use its best efforts to challenge such request to the extent possible and/or limit the response to the request to Data Subjects in the relevant jurisdiction.

Article 4. Security Obligations

4.1

Processor shall develop, implement and maintain adequate technical and organizational security measures to safeguard the security of the Personal Data in accordance with Data Protection Laws. These measures will guarantee an adequate level of security, taking into account the risks involved with the Processing and the nature of the Personal Data, prevailing industry standards and mandatory security requirements applicable to Processor. Parties acknowledge that the adequacy of the security measures mentioned in this Article 4 and Annex 4 may change over time, and that an effective set of security measures demands frequent evaluation and improvement of security measures. Processor will therefore frequently evaluate and tighten, increase or improve such measures to ensure compliance.

4.2

These technical and organizational security measures shall include, as a minimum standard of protection, the security requirements set out in Annex 4 of this DPA in order to help ensure:

- The prevention of unauthorized persons from gaining access to Personal Data processing systems (physical access control);
- The prevention of Personal Data processing systems from being used without authorization (access control);
- That persons authorized to use processing system have access only to those Personal Data they need and are authorized to access, and that Personal Data cannot be read, copied, altered or removed without authorization during Processing (access control);

– That Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the recipient entities for any transfer of Personal Data by means of data transmission can be established and verified (data transfer control);
– The establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from any processing systems (entry control);
– That Personal Data are Processed solely in accordance with the Instructions (control of instructions);
– That Personal Data are protected against accidental destruction or loss, (availability control); and
– That Personal Data collected for different purposes can be Processed separately (separation control).

4.3

Processor will, at least once a year, have its technical and organizational measures to secure the Personal Data audited by an independent third party auditor in accordance with the ISAE 3402/SOC 2 audit standard (or an equivalent audit standard selected by Processor). Processor shall, upon request from Controller, make the most current final audit report of such ISAE 3402/SOC 2 audit available to Controller for review. The ISAE 3402/SOC 2 audit will be performed by an independent professional auditing firm of good standing. Processor adheres to, and is at least once per year audited for compliance to, the PCI DSS data security and confidentiality standard. Processor will on Controller's first request demonstrate Processor's then current compliance by sharing its latest certification in accordance with this standard. Parties agree that the above-mentioned audits are the method of audit mandated by the Controller for the purpose of Article 28(3)(h) of GDPR and Clause 8.8(d) of the SCC's in Annex 6.

4.4

Processor shall ensure that any Employee entrusted with Processing Personal Data has signed appropriate confidentiality obligations and is properly instructed to perform its duties in a manner helping to ensure compliance to the terms of this DPA and has been duly instructed to apply the applicable data security and confidentiality standards.

Article 5. Personal Data Breach

5.1

In case of a Personal Data Breach, Processor shall notify Controller without undue delay, and in order for the Controller to meet its notification obligations under Data Protection Laws, after becoming aware of a Personal Data Breach. Processor shall use its best commercial efforts to address the following in the notification:

– Description of the nature of the Personal Data Breach including, where possible, the categories and number of Data Subjects;
– Name and contact details of Processor's data protection officer or other point of contact where more information can be obtained;
– Description of the likely consequences of the Personal Data Breach; and
– Description of the measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including where appropriate measures to mitigate its possible adverse effects.

Where it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5.2

Processor will promptly take the necessary and appropriate actions to investigate, mitigate and remediate any effects of a Personal Data Breach, and provide assistance to Controller to ensure that Controller can comply with specific obligations under Data Protection Laws it may be subject to in relation to the Personal Data Breach.

Article 6. Sub-Processors

Controller provides Processor hereby with a general authorization to engage Sub-Processors including those as listed online at Adyen List of Sub-processors.

Processor will impose the same material data protection obligations on the Sub-Processors as set out in this DPA, in particular in relation to the implementation of appropriate technical and organizational measures. Processor shall notify Controller of any intended changes concerning the engagement or replacement of a Sub-Processor and Controller shall be given thirty (30) days to object, duly motivated and in writing, after receiving such notification. If Processor fails to address such objection, Controller's sole and exclusive remedy is to terminate the Merchant Agreement and this DPA immediately

by providing written notice to Processor. For the avoidance of doubt, in the event Processor uses Sub-Processors, Processor shall remain fully liable to the Controller for the fulfilment of its obligations under this DPA.

Article 7. Assistance

Taking into account the nature of the Processing and the information available, Processor will provide Controller with reasonable assistance upon request with regards to (i) ensuring compliance with Controller's obligations pursuant to Data Protection Laws; (ii) making available to Controller all reasonable information necessary to demonstrate compliance with Data Protection Laws; and (iii) performing the necessary data protection impact assessments and prior consultation procedures as required under Data Protection Laws.

Article 8. Indemnification

Provided and to the extent that such breach is not caused by or attributable to Controller, Processor shall indemnify and keep Controller harmless from any claim (including reasonable legal fees) brought against Controller by a third party as a direct result of a breach by Processor of its data protection commitments in this DPA. The total liability of Processor under this indemnity provision shall be limited to three (3) times the annual Processing Fees. Controller shall promptly notify Processor in writing of any claim for which Controller believes it is entitled to be indemnified pursuant to this DPA. Processor shall immediately take control of the defense and investigation of such claim and shall employ counsel of its choice to handle and defend the same, at Processor's sole cost and expense.

Article 9. Term and Termination

9.1

This DPA shall take effect from the Effective Date of the Merchant Agreement and continue until the termination of the Merchant Agreement, after which this DPA will automatically simultaneously terminate, with the exception of the clauses which by their nature should continue to remain in full force and effect.

9.2

Processor will, upon termination or expiration of this DPA, return or delete any Personal Data on Controller's request. Processor will confirm the return or deletion of Personal Data in writing. Processor will not be required to delete Personal Data where retention by Processor is mandatory to comply with applicable legal requirements, or where retention obligations imposed by Scheme Owners apply for payment transactions using their Payment Method. Processor will in such case block the Personal Data for further use, ensure the secured storing of such Personal Data and not use such Personal Data for any other purpose than such compliance purposes. In the event deletion of a payment transaction and/or related Personal Data is not practically possible due to technical limitations or the reasonable cost associated with this deletion, Controller acknowledges that Processor may choose to use anonymization measures, rather than delete, certain Personal Data.

Annex 2 to DPA – Controller to Controller Terms

Article 1. Scope of Processing and General Obligations

1.1

For the Processing of Personal Data to which this Annex applies, Merchant and Adyen acknowledge and agree that each will act as separate and independent Data Controllers in relation to the Personal Data which they Process.

1.2

Each Party undertakes to comply with its obligations under the Data Protection Laws and will not do or permit anything to be done which might cause the other Party in any way to breach its obligations under Data Protection Laws.

1.3

In addition to Clause 1.2, Parties shall take all measures required pursuant to Article 32 of the GDPR and best industry practice to ensure the security of Processing of the Personal Data.

Article 2. Transfers

In the event of a Restricted Transfer from Merchant to an Affiliate of Adyen (meaning affiliated entities in the same corporate group as Adyen, i.e. entities Controlling Adyen, under the Control of Adyen or under common Control with Adyen) acting as a separate and independent Controller in relation to the Personal Data Processed, Adyen will ensure that the Adyen Affiliate will enter into the Controller to Controller Standard Contractual Clauses with Merchant or will, in cooperation with Merchant, take all necessary steps to put in place an alternative adequate mechanism to protect the Personal Data in compliance with Data Protection Laws.

Article 3. Assistance

Each Party shall cooperate with the other, to the extent reasonably requested, in relation to any communication from a Supervisory Authority concerning the Processing of Personal Data, any requests of Data Subjects with respect to their Personal Data Processed or compliance with the Data Protection Laws.

Annex 3 to DPA – Specific Local Requirements

In addition to Annex 1 of this DPA, to the extent applicable and for the purposes of the specific local requirement as provided in this Annex, the Parties understand and agree that these specific local requirements only apply to Adyen where Adyen acts as a Data Processor of Personal Data.

For purposes of this Annex the term Data Protection Laws specifically includes applicable federal and state laws in the United States governing the Processing of Personal Data including Civ. Code §§ 1798.100 et seq. (the California Consumer Privacy Act of 2018) ("CCPA"), the California Privacy Rights Act of 2020 ("CPRA"), Colo. Rev. Stat. §§ 6-1-1301 et seq. (the Colorado Privacy Act) ("CPA"), Connecticut's Data Privacy Act ("CTDPA"), Utah Code Ann. §§ 13-61-101 et seq. (the Utah Consumer Privacy Act) ("UCPA"), and VA Code Ann. §§ 59.1-575 et seq. (the Virginia Consumer Data Protection Act) ("VCDPA").

Article 1. Processing Requirements

1.1

Adyen will: (1) Process Personal Data only as set forth in the Agreement and this Annex; (2) Process Personal Data at all times in compliance with Data Protection Laws, including by providing no less than the level of privacy protection as required by Data Protection Laws; and (3) ensure that each person Processing Personal Data is subject to a duty of confidentiality with respect to the Personal Data. Adyen acknowledges that Merchant is disclosing, or authorizing Adyen to collect on Merchant's behalf or otherwise making available, Personal Data in connection with the Agreement only for the limited and specified purposes set out in the Agreement and this Annex.

1.2

Adyen will not (1) "Sell" or "Share" (as those terms are defined under Data Protection Laws) Personal Data; (2) retain, use, disclose, or otherwise Process Personal Data (i) for any purpose other than for the business purposes and the Services set forth in the Agreement, the DPA, or Merchant's Instructions, or as required by Applicable Laws, or (ii) outside of the business relationship between Merchant and Adyen; or (3) combine any Personal Data with Personal Data that Adyen receives from its own interactions with Data Subjects, provided that Adyen may so combine Personal Data for a purpose permitted under Data Protection Laws if directed to do so by Merchant or as otherwise expressly permitted by Data Protection Laws.

Article 2. Additional Rights and Obligations

2.1

Adyen will reasonably cooperate with Merchant in responding to individual rights requests under Data Protection Laws, by assisting with appropriate technical and organizational measures to facilitate or complete such requests, including requests by individuals to access, delete, correct, and limit the Processing their Personal Data. Where Merchant is able to effectuate any such individual request itself such as by accessing the Personal Data from the systems of Adyen through the Customer Area, Merchant will retrieve such information itself from the systems of Adyen in order to fulfill individual requests. Adyen will promptly inform Merchant in writing of any requests with respect to Personal Data.

2.2

Upon Merchant's request, Adyen will promptly delete or return all Personal Data from Adyen's records unless retention of such Personal Data is required by Applicable Law. Adyen will not be required to delete any Personal Data on archival or back up records, the deletion or return of which would be infeasible or require the use of forensic methods. Such Personal Data will be treated in accordance with Adyen's data retention policies. In the event Adyen is unable to delete the Personal Data, Adyen will (i) inform Merchant of the reason(s) for its refusal of the deletion request; (ii) ensure the privacy, confidentiality and security of such Personal Data (and the terms and conditions will continue to apply to such Personal Data); and (iii) delete the Personal Data promptly after the reason(s) for Adyen's refusal has expired.

2.3

During the time the Personal Data is disclosed to Adyen, Merchant has no knowledge or reason to believe that Adyen is unable to comply with the provisions of this Agreement.

2.4

Adyen will upon request make available to Merchant all reasonable information in its possession necessary to demonstrate Adyen's compliance with Data Protection Laws.

2.5

Merchant may, upon providing reasonable notice to Adyen, take all reasonable and appropriate steps to prevent, stop, or remediate any unauthorized Processing of Personal Data by requesting Adyen cease the Processing of Personal Data and/or cease the transfer of Personal Data to Adyen, which will not constitute a breach of the Agreement or this DPA.

Article 3. Audits

Adyen agrees to cooperate with any reasonable and appropriate assessments, or other steps to be performed by Merchant or Merchant's designated assessor that Merchant deems reasonably necessary to confirm that Adyen Processes Personal Data in a manner consistent with Merchant's and Adyen's obligations under Data Protection Laws or this Annex, including, through measures such as ongoing manual reviews, automated scans, and regular assessments, audits, or other technical and operational testing at least once every twelve (12) months. The parties agree and acknowledge that delivery of Adyen's annual ISAE 3402/SOC 2 audit report and PCI DSS Attestation of Compliance will suffice Adyen's obligations to Merchant under this Article 3 or any other similar audit requirement under Data Protection Laws.

Annex 4 to DPA – Personal Data Protection and Security Program

The measures in this Annex reflect the protections and risk mitigations in place for the systems and services processing Personal Data. Adyen commits to implement and maintain technical and organizational measures as least as stringent as those included below (details may change over time but the overall level of security will not decrease).

1. External Independent Testing and Assurance

a. Payment Card Industry Security Standards Council (PCI SSC)

- Assessed annually by a certified QSA for the PCI SSC.
- PCI program compliance:
    - PCI DSS Level 1
    - PCI PIN
    - PCI P2PE
    - PCI 3DS
- Attestations of Compliance (AoCs) are shareable upon request.

b. SOC 2 Type 2

- Assessed annually by an external auditor.
- SOC 2 Type 2 report is shareable upon request.

c. Security testing

- Continuous internal security testing.
- Continuous external independent security testing.
- Program overview is shareable upon request.

2. Information Security Program

Our commitment to data security for customers, partners, and employees is demonstrated by robust measures implemented throughout the entire lifecycle of processes, information and systems which is outlined in the information security program. This program outlines the processes and components put in place by Adyen to ensure governance and management of information security. The scope of the information security program includes all Adyen infrastructure, products, applications, software, people, vendors, office locations and data centers.

The information security program and its controls are assessed yearly by Adyen's internal audit function, PCI DSS assessment and SOC 2 Type 2 audit. The controls are further reviewed on a quarterly basis by Adyen's Corporate Risk team.

Adyen commits to implement and maintain the controls laid out in the information security program. The security program is shareable upon request.

3. Security Team

Adyen operates and maintains a dedicated information security team consisting of specialist domains: security engineering; product security; platform security; governance; risk; compliance; incident response; security culture. Adyen's head of security performs an oversight function across all the security domains and reports to multiple stakeholders, including Adyen's Chief Risk and Compliance officer (CRCO) and Adyen's Board of Directors.

4. Identity and Access Management

The following measures are in place to protect and limit access to systems processing Personal Data:

- Access is granted and maintained based on individual job function.
- All additions, changes, and deletions to individual system access is approved by a manager and must be accompanied by a business case.
- Automated Joiners-Movers-Leavers process is established to terminate all logical access to systems. This process is periodically reviewed for monitored any suspicious activity.
- The principle of least privilege is maintained throughout access management requirements.
- Access to Adyen systems processing Personal Data require an Adyen managed laptop with a pre-installed certificate, combined with multiple levels of authentication, including a hardware token for any administrative accounts.
- Unique, individual user IDs are required. By policy, shared accounts are not permitted.
- Where applicable, systems have:
    - Re-authentication after inactivity;
    - Lockout after multiple failed login attempts;
    - Password complexity requirement: 12 characters long; upper and lower case; at least one digit; at least one special character.
- User and system activity logs are monitored in accordance with Article 12 of this Annex.

5. Customer Area

Security measures are configurable by Merchant for their Customer Area. Up to date information on security measures are available publicly on Adyen Docs: https://docs.adyen.com/account.

6. Security Training and Awareness

The following security training requirements are in place:

- All Adyen employees receive security training at the point of onboarding, and annually thereafter.
- All Adyen developers require additional secure development training, and additional training annually.
- Adyen Security operates a continuous security awareness program, spreading awareness on key security topics, events and social engineering practices.

7. Data at Rest and Data in Transit

The following measures are in place to protect Personal Data at rest and in transit:

- Personal Data at rest is encrypted using industry standard encryption.
- Personal Data is protected during transit using industry standard encryption.
- Adyen implements strong encryption, data masking and/or pseudonymization of Personal Data when internally processed.
    - Personnel requiring access to Personal Data not protected as such is strictly controlled, based on need-to-know principles with monitoring of access, and data loss prevention alerting in place.
- Personal Data at rest is logically segmented from other merchant data.

8. End-User Device Data Protection

The following measures are in place to protect end-user devices:

- Disk level encryption using industry standard encryption.
- Standardized configuration in line with industry best practices.
- Not permitted to have root access.
- Anti-virus and anti-malware solutions running as standard.
    - Malware signatures are updated multiple times per day.
- Connection to Adyen network via certificate-based VPN.
- Automatic screen-lock after an idle time of 5 minutes.
- Password complexity requirement: 12 characters long; upper and lower case; at least one digit; at least one special character.
- Adyen wireless networks which end-user devices connect to are configured with WPA2 encryption.

- The connection of removable media is technically restricted and monitored.
    - Authorized use must be accompanied by a clear business case, dual permission by information security and manager, and is time restricted. At all times, data on such removable media is encrypted using file or device encryption.
- Employees are only permitted to install software from a managed environment.
    - Downloads and mounting of software outside of this catalogue is not permitted and strictly monitored.

9. Infrastructure Security

The following measures are in place to ensure infrastructure security:

- Automated configuration standards are enforced for all infrastructure components.
    - Monitoring and alerting on configuration changes and deviations from set standards.
- Network architecture segmentation into separate environments.
- Dual firewall control, at network and host level.
    - Firewall rules are tested minimum quarterly.
- Automatically enforced policy for change management, including 4 eyes principle.
- Network intrusion detection and prevention (IDS/IPS).
- Network traffic is secured with industry standard transport level security.
- All data center facilities adhere to strict requirements for physical security:
    - Physical access to the data centers is limited to Adyen authorized personnel or contractors (with direct oversight from Adyen personnel) whose job function or responsibilities require such physical access.
    - Physical access to the data centers is enforced by security checkpoints, the presence of guards, and authentication using badges and/or biometrics.
    - Access to the Adyen areas is restricted to authorized personnel through two factor authentication using badges and/or pin pads.
    - Visitors accessing data centers are accompanied by authorized Adyen personnel, and all access will be logged via the data center visitor list. Visitors are required to provide proof of identification in the form of an ID.
    - Video surveillance is in place to monitor ingress and egress of the data centers.
    - Physical access to the data centers and Adyen areas is monitored 24/7.

10. Platform Reliability

The following measures are in place to ensure platform reliability:

- Database clusters are deployed in high availability configuration.
- Adyen services are linearly scalable to meet new operational demand.
- Platform updates are released without downtime for maintenance.
- Per region, any data center can take the full load of another, including peak load.
- Global, multi-continental, dispersion of data centers. Monthly testing for data center recovery and stabilization.
- Data center data is backed up via continuous mirroring between servers and data centers. This occurs by storing complete point-in-time snapshots of a database. Snapshots are continuously captured throughout database operation.
- All data center components (hardware and software) are continuously monitored by Adyen technical support teams.

11. Cryptographic Key Management

The following measures are in place to protect cryptographic material:

- Documented, maintained and annually audited key management architecture design, procedures and processes.
- Dedicated key management expert as a part of the product security domain.
- All cryptographic keys used in encryption operations are encrypted by a key stored in the Adyen owned hardware security modules (HSMs) as a part of Adyen infrastructure.
    - Single-record encryption keys are protected using HSM keys (i.e. HSM backed).
- Process for disposing of expired cryptographic keys is aligned and audited against PCI PIN Security Standard.

– All activities surrounding cryptographic key management process directly relating to the HSMs are performed in a secure environment using key-stroke based checklists. Actions are performed by at least two people (4 eyes principle) following a set list of actions in a dedicated operations room. Access to the operations room is only accessible by two people (dual-control) for the purpose of key management.

12. Incident Response & Business Continuity

The following measures are in place to secure the continuity of critical business processes:

– Adyen maintains a business continuity management framework comprising of: business continuity policy; business impact analysis; business continuity threat and risk assessment; business continuity response plan. This framework is:
    - Designed to identify potential threats and the impacts to the continuity of business operations that those threats, if realized, might cause.
    - Subject to reviews by internal audit, to identify improvements to both the implementation and the level of resilience.
    - Tested minimum annually, with additional scoped testing weekly as a part of the platform release cycle.
    - Audited, reviewed and updated minimum annually.
– Adyen maintains an incident management framework:
    - Communicated and available to all Adyen employees.
    - Tested through internal controls by Adyen's Corporate Risk team.
    - Audited, reviewed and updated minimum annually.
    - Owned and maintained by key Adyen stakeholder.
– For incident notification information, see Article 5 of Annex 1 of the DPA.

13. Event Logging and Security Event Management

The following measures are in place to protect logs and manage security events:

– Logs generated (application, database, network, OS, platform) are stored encrypted and managed in a segmented and monitored logging cluster.
– Logs are protected from destruction and unauthorized modification.
– Logs are retained for, at minimum, one year.
– Logs are scanned first in-band and as they are consumed to the logging cluster for sensitive information.
    - In-band and cluster scanning screens for PCI sensitive data and personally identifiable information (PII).
– Adyen makes use of a security information and events management (SIEM) system supported by Adyen engineers and continuously and automatically monitored by a security duty group. This enables Adyen to detect security related events.
– Ability to carry out forensic analysis of system events.

14. Secure Software Development

The following measures are in place to ensure secure software development:

– Documented and maintained Secure Software Development Lifecycle (SSDLC) with formal development guidelines.
– Security for developers training requirement for all Adyen developers. Awareness includes:
    - Secure design principles.
    - Common secure coding vulnerabilities (e.g. OWASP top 10).
    - Topics based on industry trends, incidents, and vulnerabilities.
– Staged deployment environment where software releases are developed, tested and deployed in a weekly cycle.
– Automated and manual code reviews.
– Static code analysis.
– Dependency management.
– Secrets scanning.
– Isolated artifact management per environment (e.g. test, live).
– Threat modelling and secure design reviews.
– Ongoing (internal and external) security testing of the Adyen product and platform.
– Continuous monitoring (real-time observation, assessment, and analysis of systems, processes, or activities to detect and respond to changes, deviations, or potential risks).

15. Vulnerability Management

The following measures are in place to manage vulnerabilities:

- Vulnerability management process comprising identification, classification, prioritization and mitigation of vulnerabilities associated with Adyen systems.
- Maintain the ability to respond to critical threats at any time (24/7/365).
- Application and network vulnerability scans are conducted multiple times per month.
- Monthly external vulnerability scanning performed by a Payment Card Industry (PCI) certified vendor.
- Digesting a range of external cyber threat intelligence resources and building detections for relevant threats.
- Mitigation of DDoS attacks:
    - Utilize a bespoke anti-DDoS partner.
    - Utilize multiple content delivery networks.
    - Utilize a diverse network of internet service providers.
    - Mitigation built into the platform network architecture through geographically dispersed infrastructure.
- Unauthorized use of hardware and software are detected automatically across the Adyen infrastructure, including workstations.
- Minimum weekly system patching of all core infrastructure components, while maintaining the capability to release immediate patches.
- Ongoing (internal and external) security testing of the Adyen product and platform with a documented process for remediation of findings.

16. Data Retention, Minimization and Erasure

Adyen has a retention obligation to store all transaction data in accordance with Applicable Law. Under Dutch law, Adyen N.V. is required to store transaction data for 7 years. Stored data is only used for compliance with applicable legislation, scheme rules compliance purposes and for use in accordance with instructions from the Controller.

Adyen provides export functionalities to merchants in the Adyen Customer Area as well as manual and API options for Subject Erasure Requests.

Adyen follows the schemes and/or other applicable protocols dictating the necessary data in order to process a transaction.

Under the explicit instructions of the Merchant, Adyen processes the necessary information required from the shopper to process payment transactions. Merchants decide on the payment methods and whether to collect data beyond the minimum required data field.

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to assist the controller and, for transfers from a processor to a sub-processor, to the data exporter.

- Processing of Personal Data will be carried out by sub-processors of Adyen in accordance with the DPA and the measures as set out in this Annex;
- With respect to employee contracting and supervision.

Annex 5: Description of Processing

Subject Matter, Nature and Duration of the Processing:

The subject matter, nature and duration of the Processing of the Personal Data are set out in the Merchant Agreement.

Adyen acts as a Processor when providing the Adyen Services to the extent Adyen is following the Instructions of the Merchant. The processing is made for the following purposes:

To deliver the services under the Merchant Agreement, which include:

- Processing of payment transactions and support related services;
- Fraud detection;
- Defending charge-backs; and
- Reporting and Adyen Customer Area.

In order to initiate a payment, the following payment details (which include Personal Data) may be Processed by Adyen:

Strongly depends on which payment methods Merchant wishes to offer and the services Merchant purchases from Adyen. Categories of data; name, billing address, delivery address, email address, IP address and payment details.

Payment requests could include the following:

- Credit/debit cards
    - Card details such as CVC, expiry month, expiry year, cardholder name, card number, issue number
- Bank transfer
    - Bank account number, BIC, Bank Name, Bank Location ID, Bank Name, Country Code etc.
- Fraud detection
    - Payment details
    - Shopper name
    - Device fingerprint
    - Persistent cookie
    - Shopper email
    - IP address
    - Shopper reference
    - Telephone
    - Billing address
    - Delivery address
    - Other data Merchant elects to provide Adyen such as basket info, browser language, delivery method, shopper country etc.