StoreFeeder
multi channels ● one solution

UPDATED STOREFEEDER GDPR COMPLIANCE STATEMENT

Version: V2.0

Revision History:

Version	*Revision Date*	*Revised by*	*Section Revised*
V1.0	20-05-2019	Iain Thomson	GDPR Compliance Statement released
V2.0	08-01-2020	Iain Thomson	Updated GDPR Compliance Statement released

1. Information Security Group (ISG) - Building the right Team

a. **Team Profile:** (**Art. 37**) Identified the right senior stakeholders from across our business to ensure the correct skills are always available to develop the policies, procedures, and processes necessary to define, deploy, monitor and review work undertaken

b. **Security:** (**Art. 32**) We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality. (See points 3 (a-e) and 5 (Technical response table) for a more detailed explanation).

c. **Setting A Clear Direction of Travel**: Aligning everyone to a common set of goals and direction. [ISO27001 Compliance]

d. **Resource**: Ongoing commitment and drive to maintain a pro-active, threat detection and prevention approach to help secure resources and funding.as required

2. Raising awareness and identifying risks

a. **Employee Training –** (**Art. 5**) At StoreFeeder, we understand that we handle our Merchants, customer personal data. As a result, our staff training is a logical prerequisite for compliance with the requirements of the GDPR. In this way, our employees learn how to recognize personal data, separate it from security issues and company secrets, and develop a special sensitivity in handling personal data.

b. **Process Mapping** (**Art. 30**) - Identifying and maintaining an ongoing comprehensive inventory of our data, classification by risk and type, and data flows.

c. **Privacy Risk Assessments and Mitigation -** Using processing mapping and Data Protection Impact Assessments (DPIA) (**Art. 35**) to maintain a detailed review of privacy risks across StoreFeeder. The findings of the process mappings and DIPA's are fed into our Information Security Group (ISG) to enable us understand areas of possible improvement and identify the resource required to mitigate any risks identified.

d. **Communications:** Internal communications channel in place to maintain an internal awareness of the importance of information security.

3. Design and Implement Operational Controls

a. **Privacy Governance:** (**Art. 5**) Implementing and enforcing policies, procedures and processes necessary to monitor and investigate work undertaken within the business as defined by our information security team. [**Not an exhaustive list of policies:** IT Security Policy, (SAR) Subject Access Request Policy (**Art. 15**), Data Protection Policy, Data Retention Policy (**Art. 5**), Data Breach Policy (**Art. 33**), HR Privacy Notice, Cookies & Privacy Policy (**Art. 30**)]

b. **Privacy by Design:** (**Art. 25**), Data protection is taken into account at all stages of our development life cycle to ensure that the proportionate level of security is taken into account at any phase of the products life cycle. [See section 2.c. Data Protection Impact Assessment (DPIA)]

c. **Privacy by Default:** (**Art. 25**) Implemented appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This is done via (RBAC) Role Based Access Control in place across our network infrastructure. This is reviewed on an ongoing basis via the Information Security Group (ISG) [**See section 1**] to ensure that staff have the required access rights to support their roles. This is then enforced using Azure Active Directory. For managing resources in Azure, we've implemented RBAC controls to restrict access to resources based on the roles of employees (principle of least privilege). All developers have at least read-only access to Azure resources. As an extra layer of security, we also use two factor authentications to re-enforce (RBAC). Anomalous usage patterns are monitored via Microsoft Azure alerts and reviewed within the Information Security Group (ISG).

d. **Penetration testing:** (Art. 32) Regularly testing our IT Systems and web application to find security vulnerabilities that an attacker could exploit on an annual basis or after any major development release, via an independent 3rd party. Issues identified are built into our ongoing software development plan according to their risk rating given by the 3rd party.

e. **Individual Data Rights & Remedies of Our Merchants Customers-** (Art. 15) GDPR brought in an expansion of individual data subjects rights regarding Personally Identifiable Information (PII). At StoreFeeder, we receive (PII) from Merchants that use our service that relates to their customers and is required by us to enable the fulfilment of an order. In this situation the Merchants are the Data Controllers of their customers' data. StoreFeeder are Data Processors in this instance. To enable Merchants to fulfill their obligations under GDPR, we have provided our Merchants with the ability to delete or anonymise their data via their account settings.

4. Demonstrating Ongoing Compliance

a. Transparency: (Art. 5) Clear and simple explanations of our obligations under GDPR are displayed in our Privacy Notice and Terms and Conditions.

b. **Internal Information Audit plan (GDPR):** At StoreFeeder, we undertake information audits covering points 1-4 listed in this compliance statement to provide management with an evaluation of how effectively GDPR is being governed, monitored and managed. The audits focus on GDPR governance and response mechanisms as well as supporting processes, which can help to manage the risks associated with non-compliance to GDPR.

5. Technical Response Table:

A more technical answer to frequently asked questions asked to date

	Question	Response
1	**Acceptable Use**	
1.1	Do you use Personally Identifiable Information (PII) for any purpose other than Shipping labels and/or tax purposes?	No – data provided by our Merchants is used only for order fulfilment and tax purposes.
1.2	Where geographically do you host data?	Data is primarily stored in Azure **West Europe (Netherlands)** and backed up to **Azure North Europe (Ireland)**
1.3	Merchant information that we collect, read, store, share and amend.	**[Courier Integrations]** 13ten, amazon logistics, DHL, DPD, DPD Local, DX, FedEx, Hermes, Huxloe logistics, MetaPack, netdespatch, Parcel Force, Parcel Station, Royal Mail. For courier integrations we only provide information that is pertinent to the creation of labels. Addresses and Customs information. **[Accounting Integrations]** KashFlow, Tradebox, Xero. We send information for tax purposes to the account packages of kashflow, tradebox and xero. This is payment information, product and address information.
2	**Network Protections**	
2.1	How is your infrastructure hosted (e.g. on-premise, AWS, Azure cloud solution)?	We use Microsoft Azure, an ISO/IEC 27001 certified partner. Currently, Azure Public are audited once a year for ISO/IEC 27001 compliance by a third-party accredited certification body, providing independent validation that security controls are in place and operating effectively
2.2	How do you restrict network-level access to your infrastructure (web servers, database servers, endpoints, etc)?	Network access to databases are restricted to whitelisted IP-address, username and password. Staff have (RBAC) Role Based Access Control. This is reviewed on an ongoing basis via our Information Security Group (ISG) to ensure that staff have the required access rights to support their roles. Login attempts are limited to 5 attempts. Anomalous usage patterns are monitored via Microsoft Azure alerts and reviewed within our Information Security Group (ISG). Frontline Customer Data Support staff can only temporarily access customer data if the authorised account holder permits it as part of our Data Protection Identify verification process and it is required to enable the resolution of the account holders query.
2.3	Do you restrict public access to your database/file servers and desktop/developer endpoints? If so, how?	Yes. Network access to databases are restricted to whitelisted IP-address, username and password. Staff have (RBAC) Role Based Access Control. This is reviewed on an ongoing basis via the Information Security Group (ISG) to ensure that staff have the required access rights to support their roles. As an extra level of security, personally Identifiable information is also hidden from staff via data masking.

3	Data Access Management	
3.1	Access management overview	Staff have (RBAC) Role Based Access Control. This is reviewed on an ongoing basis via the Information Security Group (ISG) to ensure that staff have the required access rights to support their roles. This is then enforced using Azure Active Directory. For managing resources in Azure, we've implemented RBAC controls to restrict access to resources based on the roles of employees (principle of least privilege). All developers have at least read-only access to Azure resources. As an extra layer of security, we also use two factor authentications to re-enforce (RBAC). If an employee needs to access a production resource they must consult with our DevOps Engineers who will decide whether access is necessary, or whether the task can instead be managed by the DevOps Engineers (preferred option). Anomalous usage patterns are monitored via Microsoft Azure alerts and reviewed within the Information Security Group (ISG).
3.2	Have you assigned a unique ID (for logging and accountability) to each employee who has access to Merchants Information?	Yes, we log the member of staffs email address every time they access any data on the system. We also have data masking enabled at database level so that staff cannot access personally identifiable information. If an employee needs to access a production resource they must consult with our DevOps Engineers who will decide whether access is necessary, or whether the task can instead be managed by the DevOps Engineers (preferred option).
3.3	How often do you review (and baseline) access to Merchant Information?	We have a monthly information security group meeting. Where we discuss any changes to access that is provided to staff or any changes to functionality that require discussion or changes to process. The Information Security Group is not the only forum though. If staff have concerns or during the planning, designing and implementing of a new feature a concern is raised then ad hoc meetings will take place as required to ensure that we are always following best data practices.
3.4	Do you have a lockout mechanism in place when a malicious activity or log-in attempt is detected?	The number of logins are limited, database IP addresses are restricted and unusual activity is monitored with azure alerts. With auditing, we can then drill down and investigate. Anomalous usage patterns are monitored via Microsoft Azure alerts and reviewed within the Information Security Group (ISG). We also have alerting set up for number of failed requests to our services. When these go above baseline levels they are investigated by Senior DevOps Engineers to look for malicious actions. If our software performance levels are not operating within expected parameters, our DevOps engineers will investigate and identify the reason for this deviation. If required DevOps engineers can intervene and adjust or use the equivalent of a 'kill switch' for any internal or customer process that is adversely affecting overall software performance.
3.5	Do you keep an inventory of asset hardware and software that stores Merchants information?	Yes. We use Microsoft Azure cloud services for storage of all Merchant data.
3.6	Do you allow employees to store Merchants data on personal devices?	No.
3.7	Do your access controls divide data access between PII and non-PII access?	Yes. Employees are only allowed read only access to Merchants data and when it is personally identifiable information it is data masked.
4	Encryption in Transit	
4.1	Are you encrypting all data-in-transit for all internal and external endpoints? Please specify any data transfers, internal or external, which are not encrypted.	All data that is accessed in transit is served over HTTPS. All data at rest is encrypted. Encryption keys are only stored in Azure KeyVault.

5	**Incident Response Plan**	
5.1	**1) Threats can be identified via the following paths:** a) **Microsoft Azure Threat Detection Alerts:** Are monitored throughout the day to identify any anomalous usage patterns. Alerts are sent to **Incidentalerts@storefeeder.com.** This is a monitored email box. b) **Detected during software development:** Our Developers identify incidents whilst undertaking day to day software development. This would be reported to Our Lead Developers to identify if intervention required. If it is , a notification would be sent to **Incidentalerts@storefeeder.com** detailing the type of incident that had occurred and action taken to resolve it. c) **Incident is reported by an external source:** Details are to be forwarded to **Incidentalerts@storefeeder.com.** We also intend to introduce the use of **securitytxt.org** to allow security risks identified in web services discovered by independent security researchers who understand the severity of the risk, a secure channel to disclose them properly to us thus avoiding identified threats being left exposed due to the lack of a secure channel to notify us by. 2) **Who to notify:** As soon as a data security incident has been detected, it is reported to **Incidentalerts@storefeeder.com.** This email group consists of our Lead DevOps, Software Development Manager, Compliance Manager, IT Manager and Managing Director. 3) **Analysis:** This group is responsible for reviewing and investigating the incident to ascertain whether or not a data breach may have occurred or still be ongoing regardless of the severity, impact or subsequent containment of the security incident. All data security incidents are reported to and logged by this group with immediate effect. As soon as an incident has been reported, initial assessments are made, and trends identified where possible and where appropriate resources are allocated and measures must be taken to contain the incident. Such measures are not in the scope of this description due to the vast nature of security incident that could occur and the variety of measures that could be take. Each month a review is undertaken of all reported incidents and reviewed within The Information Security Group (ISG) to ensure that appropriate threat patterns are being identified and mitigating actions undertaken. 4) **ICO Notification**: Where a security incident is found to involve a breach in personal data, The Compliance Manager will notify The (ICO) Information Commissioners Office within 24 hours of this discovery and provide the ICO with a summary of our investigations and findings so far - this will be sent via the ICO reporting service at: https://report.ico.org.uk/security-breach/	
6	**Data Governance**	
6.1	External Privacy policy:	https://storefeeder.com/Company/Privacy-Policy
7	**Encryption and Storage**	
7.1	Are you encrypting all data-at-rest, including data backups?	Yes - data at rest and backups are encrypted. By default, data written to Azure is encrypted when placed on disk and decrypted when accessed using Azure Storage Service Encryption, Azure Key Vault, and Azure Active Directory (which provide secure, centrally managed key management and role-based access control, or RBAC).
7.2	What protocol are you using to encrypt data-at-rest?	Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption and is FIPS 140-2 compliant. By default, data written to Azure is encrypted when placed on disk and decrypted when accessed using Azure Storage Service Encryption, Azure Key Vault, and Azure Active Directory (which provide secure, centrally managed key management and role-based access control, or RBAC).
8	**Least Privilege Principle**	
8.1	How does your organization follow the principle of least privilege to ensure that access to PII is granted on a "need-to-know" basis?	If an employee needs to access a production resource they must consult with our DevOps Engineers who will decide whether access is necessary, or whether the task can instead be managed by the DevOps Engineers (preferred option). Anomalous usage patterns are monitored via Microsoft Azure alerts and reviewed within the Information Security Group (ISG).

9	Logging and Monitoring	
9.1	How are you generating logs?	We generate logs the following ways: 1. We have general IIS and server agent logs. 2. We have azure application insights which provide exception logging. 3. We use the ELK stack for our logging purposes. This allows us to log pertinent information. 4. Database Auditing 5. General settings auditing within the application stored in the users database We use azure security centre to notify us of intrusion attempts or unusual usage.
9.2	Are you logging security-related events (like access and authorization events, intrusion attempts, configuration changes, etc.)?	• Every database has auditing turned on so we can see all access attempts and who has accessed what. • We also log who has accessed every page in the system. • We also log login attempts and lock people out after 5 unsuccessful attempts • System settings changes are also logged with which user updated them
9.3	Are you storing PII in logs?	No.
9.4	Do you have mechanisms in place to monitor the logs and trigger alarms in case of malicious activity?	• We have threat detection and auditing turned on at the database level. • We have azures built in unusual activity detectors and cloudflare. • We also have azure security centre enabled.