Dutchview
INFORMATION TECHNOLOGY

Dutchview's NIS2 Answers on Customer questions

Version 1.0, October 2024

Since 2019, Dutchview has been ISO 27001 certified, demonstrating our commitment to maintaining a robust information security management system. This certification covers a significant portion of the requirements outlined in the NIS2 directive, ensuring that we have established effective processes and controls to protect our information assets. Below, we present a series of questions and answers that illustrate how Dutchview complies with the NIS2 guidelines.

#	Question/Answer
1.	**How does Dutchview assess the IT infrastructure for vulnerabilities?**
	Dutchview conducts a quarterly information security audit, assessing incidents and implementing corrective and preventive measures. Additionally, various aspects of information security are continuously monitored. **Methodology** The organisation employs manual evaluations of configurations, code, and infrastructure conducted by security experts. Regular internal penetration tests are carried out, and an independent external party is engaged annually for a pentest, primarily following the OWASP Top 10 guidelines. **Risk Management and Prioritization** Identified vulnerabilities are included in a Risk Treatment Plan, where the likelihood and impact of each risk are assessed to determine the overall risk. The security team then prioritises these vulnerabilities based on their likelihood, impact, and the effort required to address them, ensuring that resources are allocated effectively to mitigate potential threats. **Responsibilities** The security team, including the security officer and privacy officer, is responsible for conducting vulnerability assessments. Follow-up on findings is delegated to the responsible departments, with progress being closely monitored. **Training and Awareness** Staff is trained through an internal newsletter, monthly meetings, and mandatory security and privacy awareness training tailored to their roles. **Documentation and Reporting** Quarterly reports are prepared and shared with stakeholders, while the rest of the organisation is informed via the internal newsletter and monthly meetings.

#	Question/Answer
2.	**Is antivirus software and a firewall being used, and are log files available for this?**
	Yes, Dutchview utilises antivirus software and a firewall for system and network protection. **Antivirus Software** Dutchview uses antivirus software to provide comprehensive protection against malware and other threats. **Firewall** A software-based firewall is in place both on our servers and on individual workstations to safeguard the network and systems from unauthorised access and potential threats. Log files on the server side are maintained, and access is restricted to a select group of employees who have permissions to those servers. Both antivirus and firewall systems on workstations are equipped with logging mechanisms and alert systems. These logs, as well as the alerts generated by these systems, are accessible to only one designated employee within the organisation, ensuring strict control over access and monitoring. This setup guarantees that security information remains tightly managed while maintaining compliance with relevant security standards.
3a.	**How are the backups managed?**
	Dutchview has a comprehensive backup strategy to ensure the security and availability of customer data and internal environments. **Backup Frequency** Customer data (Production) is backed up daily, weekly, and monthly, covering a retention period of six months. Internal Development/Test/Acceptance environments are backed up daily or weekly, depending on the associated risk. **Backup Location** Daily and weekly backups are stored in Frankfurt, Germany, while monthly backups are stored in Dublin, Ireland—all within the EU. **Encryption and Security** Backups are stored in separate accounts (sandbox), and access is restricted to limited users within the organisation.

#	Question/Answer
	Recovery Procedure According to the Disaster Recovery Plan, Dutchview has a Recovery Point Objective (RPO) of a maximum of 24 hours. This means that data will be restored to a state no older than 24 hours before a disruption occurs, with much of the data also being automatically resynchronised. Additionally, the Recovery Time Objective (RTO) is set at a maximum of 24 hours, ensuring that systems and operations can resume swiftly within this timeframe following any data loss or system failure.
3b.	**Is the restore process also practised?**
	Yes, backups are tested at least once every quarter or every six months, depending on the associated risks, to verify that they can be restored correctly.
4a.	**How are our customer data and systems protected against cyber threats such as ransomware and phishing?**
	Dutchview has implemented several measures to protect customer data and systems against cyber threats, including ransomware and phishing. **Security Measures** ● Multi-Factor Authentication (MFA) and Single Sign-On (SSO) are required wherever possible to secure access to systems. ● Dutchview's email provider has built-in spam and phishing filters that automatically detect suspicious messages. ● Employees undergo regular awareness training and are granted access to data and systems only after obtaining the necessary certifications. ● Application logs and infrastructure logs are stored securely and exceptions are notified. ● Application and data backups are being maintained in the sandbox network. **Monitoring and Detection** Dutchview has an incident response plan in place that outlines how to respond to suspicious activities, including communication and escalation procedures. Suspicious activities are automatically reported to system administrators for further assessment. **Preventive Measures** ● Systems and applications are configured according to security guidelines and best practices to minimise vulnerabilities. ● The security team is closely involved in software development by conducting security testing and code reviews, as well as participating in the pre-development phase (design).

#	Question/Answer
	• Employees receive simulated phishing emails regularly to increase their awareness of these threats. **Evaluation and Improvement** Regular internal and external audits are conducted, leading to points for improvement, thereby continually evaluating and enhancing the effectiveness of the measures taken.
4b.	**And where is the data stored?**
	Data is stored in the EU, Germany (Frankfurt)
5.	**Is the data stored encrypted, and can personal data be deleted if desired?**
	Yes, Dutchview employs several measures to ensure the security of data storage and the management of personal data: • **Encryption of Data at Rest**: This remains an ongoing area of focus, and we are continually investing effort into further improving these encryption measures. • **Encryption During Transmission**: Personal data is encrypted during transmission (in transit), ensuring that data remains secure as it moves between systems. • **Policies for Encrypting Sensitive Data**: There is an information security policy in place that guides the categorisation of data based on its sensitivity, leading to decisions on appropriate encryption methods for sensitive data. • **Deletion of Personal Data**: Individuals have the right to delete their personal data. They can either delete their data themselves or request Dutchview to do so. • **Process for Data Deletion Requests**: A formal process exists to handle data deletion requests. Only administrators can initiate these requests, and they must confirm the request via email to ensure proper verification of identity. • **Retention Periods for Personal Data**: Retention periods for personal data vary according to the sensitivity of the data. The periods are designed to be shorter or longer based on the specific requirements of the data. • **Data Breach Response Plan**: Dutchview has a data breach response plan that includes procedures for handling unencrypted personal data in the event of a breach, ensuring a comprehensive approach to data security.
6.	**Have the latest security updates been installed on all programs?**
	Security updates and patches are monitored using specialised tools and are installed on servers shortly after their release. As for workstations, employees are expected to keep their devices up to date either automatically or, if automatic updates are not possible,

#	Question/Answer
	manually. This requirement aligns with the rules outlined in our information security policy.
7.	**How are Dutchview's passwords and multi-factor authentication secured?**
	Dutchview ensures that both passwords and multi-factor authentication (MFA) are secured through several best practices and tools: **Password Security** • Passwords are required to meet system-enforced complexity standards, such as a minimum of twelve characters. • For one-factor authentication, passwords expire after six months, ensuring regular password rotation. • Passwords are protected through encryption during both transport and storage to prevent unauthorised access or tampering. • Dutchview uses a password management system, which employs strong encryption to securely store passwords and utilises a zero-knowledge architecture, meaning even the service provider cannot access stored passwords. **Multi-Factor Authentication (MFA)** • Two-factor authentication (2FA) is enforced wherever possible, utilising authentication apps or SMS to provide an extra layer of protection. • Single sign-on (SSO) is also implemented when supported, simplifying the login process while maintaining high security standards. By following these protocols, Dutchview ensures that access to systems and data is highly secured against unauthorised use.
8.	**What actions are taken when Dutchview is hacked and you as a customer are involved?**
	When Dutchview experiences a cyberattack that potentially involves customer data, the following actions are taken: • **Incident Response Plan**: Dutchview has an incident response plan that provides clear guidelines for handling cyberattacks. • **Customer Communication**: Customers are promptly informed about the nature of the attack and the data that may have been exposed. • **Evaluation and Improvement**: After an incident, an evaluation is conducted to determine what went wrong and what improvements can be made to prevent recurrence.

#	Question/Answer
	• **Audits and Monitoring**: Regular internal and external audits are performed to assess the effectiveness of the incident response plan and address any shortcomings. • **Incident Tracking**: Procedures are in place for documenting security incidents and the subsequent actions taken. These measures ensure that Dutchview can respond adequately to security incidents and minimise the impact on customers.
9.	**How does Dutchview report security incidents?**
	Dutchview has established a comprehensive process for reporting security incidents, which includes the following key steps: • **Internal Reporting**: Employees are encouraged to report any security incidents or suspicious activities immediately through established internal channels. • **Incident Documentation**: Each reported incident is documented in detail, including the nature of the incident, affected systems, and any immediate actions taken. This documentation helps in assessing the impact and determining the next steps. • **Assessment and Analysis**: Once an incident is reported, it is assessed by the security team. This includes analysing the incident to understand its cause, scope, and potential impact on the organisation and its customers. • **Notification of Stakeholders**: Depending on the severity and impact of the incident, relevant stakeholders, including management and affected customers, are notified. Communication is done in a transparent manner, outlining the incident's nature and the steps being taken to mitigate its effects. • **Compliance with Regulations**: Dutchview ensures that incident reporting complies with relevant legal and regulatory requirements, such as GDPR and the NIS2 Directive, which may require notifying authorities and affected parties within specific timeframes. • **Post-Incident Review**: After an incident has been resolved, a post-incident review is conducted to evaluate the response and identify lessons learned. This review informs future incident response strategies and helps enhance the overall security posture. These structured processes ensure that Dutchview can effectively manage security incidents and communicate promptly with stakeholders, thereby minimising potential damage and maintaining trust.

Please also check our NIS 2 Compliance Statement