nPlan

nPlan Limited
nPlan Data and Cloud Hosting Policy

Contents Page

This Data and Cloud Hosting Policy ("the **DCH Policy**") applies to nPlan Limited and our related entities (“nPlan”, “us”, “we” and “our”) and details our commitment to protecting the data and security of our customers and users.

The DCH Policy consists of the following policies:

- Data Protection Policy
- Risk Assessment Policy
- Physical Security Policy
- Vendor Management Policy
- [Service Level Policy]

Data Protection Policy

1. Introduction

1.1 The Data Protection Policy applies to all data collected by nPlan from employees, candidates, users, customers, vendors, or other parties that provide information to nPlan, including anyone with whom nPlan collaborates with, or who acts on nPlan’s behalf, for the purposes of nPlan providing products and services.

2. Data Protection

2.1 As part of providing nPlan products and services, nPlan obtains and processes information or data. Data is hosted in our data centre in the Netherlands unless otherwise specified in the Ordering Document. We also have a data centre in the UK available for use.

2.2 nPlan retains information and data from you where we have an ongoing legitimate business need to do so (for example, to provide nPlan products and services, or to comply with legal, accounting, tax, or regulatory requirements).

2.3 nPlan commits to ensuring that information and data that you have provided is:

- Accurate and kept up-to-date
- Collected fairly and for legitimate business purposes only
- Protected against any unauthorised or illegal access by internal and external parties

2.4 Data retained by nPlan will not be:

- Communicated informally
- Stored for more than the amount of time specified in our Master Services Agreement, Privacy Policy, customer contracts, or other binding agreements
- Downloaded to unapproved devices

- Transferred to organisations, states, or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

2.5 In addition to ways of handling the data, nPlan has direct obligations towards people to whom the data belongs. Specifically we must:

- Let people know which of their data is collected
- Inform people about how nPlan will process their data
- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted, or compromised data
- Allow people to request that nPlan modifies, erases, reduces, or corrects data contained in its databases within legal guidelines specified by company policies or law-enforcement agencies

2.6 To exercise data protection we're committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Communicate how nPlan handles data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

3. Data Classification

3.1 "Customer-Confidential Data" is information that, if made available to unauthorised parties, may adversely affect nPlan customers. This classification also includes data that nPlan is required to keep confidential, either by law or under a confidentiality agreement with non-customer third parties, such as vendors. This information is to be protected against unauthorised disclosure or modification. Customer-Confidential Data is used only when necessary for business purposes with the permission of the customer and is protected both when it is in use and when it is being stored, processed, or transmitted.

4. Encryption and Cryptography

4.1 nPlan complies with industry standards for Encryption and Key Management and requires the same from all nPlan employees, contractors, and third party vendors when sensitive data is in scope, such as customer data and nPlan secrets.

4.2 All sensitive data in transit and at rest are encrypted using strong, industry-recognized algorithms.

4.3 nPlan maintains approved encryption algorithm standards. These internal standards are reviewed and subject to change when encryption standards within the security industry significantly change.

4.4 nPlan will not engage in "roll-your-own" encryption, algorithms, or practices and will not use "security through obscurity" within production infrastructure or applications.

5. Data in transit

5.1 The minimum acceptable TLS standard in use by nPlan is TLS v1.2.

5.2 All nPlan public web properties, applicable infrastructure components and applications using SSL/TLS, IPSEC and SSH to facilitate the encryption of data in transit over open, public networks, must have certificates signed by a known, trusted provider.

6. Data at rest

6.1 The use of the Advanced Encryption Standard (AES) or stronger is used for symmetric encryption.

6.2 Ciphers in use meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalogue, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation.

6.3 Algorithms in use meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms or stronger is used for asymmetric encryption.

7. nPlan Encryption Key Creation & Storage Standards

7.1 Encryption Keys generated, stored, and managed by nPlan must be generated and stored in a secure manner that prevents loss, theft, or compromise.

7.2 Key generation is seeded from an industry standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

8. Backups

8.1 All original (non-derived) customer data on infrastructure operated by nPlan is backed up.

8.2 nPlan configures full, daily database backups for all data stored by its cloud services provider. If a database instance is deleted, all associated backups are also automatically deleted.

8.3 Backups are periodically tested by the nPlan engineering team.

9. Data Deletion

9.1 The following describes how customer data is deleted in connection with the cancellation or termination of an nPlan account and applies to all data stored by nPlan except:

- data that resides in third-party services managed and hosted by third parties, with the exception of nPlan's infrastructure provider
- data that resides in nPlan products or services that are in beta, testing, or an early access program

9.2 It is nPlan's policy to store data indefinitely so that it is able to reproduce and address issues with its artificial intelligence models.

9.3 nPlan provides the option for customers to delete data after their subscription ends. This request must be made by the customer, and nPlan may require additional ID verification. All information is then deleted from production systems within two calendar quarters of the deletion request.

Physical Security Policy

1. Introduction

1.1 nPlan's Physical Security Policy describes how staff should permit access to and secure the nPlan office.

2. nPlan security team and roles

2.1 The Information Security Team is composed of individuals that manage the day-to-day compliance and monitoring activities necessary to achieve, maintain, and improve the ISMS to meet the Information Security Objectives.

2.2 The Information Security Team members are comprised of the following roles:

- CTO
- Systems & Network Administrator(s)
- Senior Engineer(s)
- Operations Director or other members of the Operations team (as needed)

2.3 nPlan requires regular security training for all staff and everyone is responsible for contributing to security.

3. People operations security

3.1 Background screens: all nPlan employees undergo reference checks prior to gaining substantial access to customer data systems. nPlan may rescind an employee's offer letter if their background check is found to be falsified, erroneous, or misleading.

3.2 Security awareness training: nPlan employees and contractors are provided training on the nPlan's security policies and procedures during their first 30 days of employment and annually thereafter. All nPlan personnel are then required to confirm that they have attended the training and understand the security policy.

3.3 nPlan employees in developer roles are supported to avoid common coding vulnerabilities. Secure coding techniques are encouraged by ongoing peer reviews, secure development guidelines, PR reviews, and learning from SDLC & other practices in the team.

3.4 Employee Acceptance of Policies: all of nPlan's security policies, including the Data Protection Policy and other policy controls supporting this Cloud Hosting Policy, are presented to new employees during onboarding, and all employees are required to sign off that they have read all such policies.

4. Physical office access

4.1 Physical access to nPlan's office is restricted using key cards for which only nPlan employees and building staff have access. nPlan reviews key card access periodically when employees leave to ensure access is restricted to current staff only.

5. Security surveillance

5.1 nPlan's office building has security cameras. nPlan has an agreement in place with building management to access camera footage in the event that it is needed.

6. Visitor access policy

6.1 nPlan employees may invite visitors to the office. nPlan staff must escort and supervise their visitors at all times and are responsible for the visitors' behaviour while they are in the office.

7. Contractors and service vendors

7.1 Contractors, suppliers and service vendors, e.g. IT technicians, may enter nPlan's office to complete their job duties. The visitors' hosts are responsible for providing contractors and vendors with appropriate identification and direction while on nPlan's premises.

8. Securing physical laptops

8.1 All employees are required to secure their physical laptops in the following manner:

- The confidentiality, security and privacy of nPlan's customers must be preserved, by ensuring that no unauthorised individuals may view, overhear, or otherwise have access to nPlan's customer data.
- To enforce, all nPlan employees are required not to view customer support emails and data, or teleconference with customers in public areas.
- All nPlan end user devices, such as laptops and cell phones containing access to internal nPlan resources, must be protected at all times and may not be left unattended.

Business Continuity Policy

1. Introduction

1.1 This plan identifies key resources and needs to ensure that business may continue, perhaps in a limited capacity, in the event of a disaster. The plan includes information such as key suppliers, contingency plans and alternative business location.

2. Key Vendors - Contacts and Contingency Plans

2.1 nPlan's core business runs across different infrastructure offerings on Google Cloud Platform (GCP).

2.2 If an outage is suspected, the GCP status page is visited to see if there is a previously known issue. If no known issue is present or a possibility for nPlan, a support ticket is submitted to GCP.

2.3 Please see the Disaster Recovery Plan section for general and detailed action plans in case of various potential GCP outages and service disruptions.

2.4 nPlan uses Zendesk for some customer support functions. If an outage is suspected, the Zendesk status page is visited to see if there is a previously known issue. If no issue is found, a support ticket is submitted to Zendesk. Email (via Google Workspace) can be used as an alternative to provide customer support in the event of an outage of Zendesk.

3. Disaster Recovery Plan

3.1 nPlan employs a Disaster Recovery Plan ("DRP") to establish procedures to recover nPlan operations following a disruption resulting from a disaster. The types of disasters contemplated by this plan include natural disasters, political disturbances, man-made disasters, external human threats, and internal malicious activities.

3.2 nPlan performs testing of the Disaster Recovery Plan annually, and the plan is updated at least annually with additional playbooks taking into account new risks of disasters learned through testing and re-enactment of past disaster incidents.

3.3 The plan includes all resources and processes necessary for service and data recovery, and covers all information security aspects of business continuity management. It ensures that all equipment, software and data (or their backups/failovers) are available in some manner and that if an incident takes place at the organisation's physical location, all resources involved in recovery efforts are able to be transferred to an alternate work site (such as their home office) to complete their duties.

3.4 This plan does not cover the following types of incidents:

i. Incidents that affect customers or partners but have no effect on nPlan's systems. In this case, the customer must employ their own continuity processes to make sure that they can continue to interact with nPlan systems.
ii. Incidents that affect cloud infrastructure suppliers at the core infrastructure level, including but not limited to Google, Slack, and Amazon Web Services. nPlan depends on such suppliers to employ their own continuity processes.

3.5 From a disaster recovery perspective, nPlan defines two categories of systems:

i. Non-Critical Systems: These are all systems not considered critical by the definition below. These systems, while they may affect the performance and overall security of Critical Systems, do not prevent Critical Systems from functioning and being accessed appropriately. Non-Critical Systems are restored at a lower priority than Critical Systems. Examples of Non-Critical Systems include analytics servers.
ii. Critical Systems: These systems host application servers and database servers or are required for the functioning of systems that host application servers and database servers. These systems, if unavailable, affect the integrity of data and nPlan aims to restore them, or have a process begun to restore them, within seven days of becoming unavailable.

3.6 Production infrastructure is considered to be critical for nPlan business operations and nPlan aims to restore it within seven days.

3.7 While specific playbooks are available for specific scenarios, there are overall rules of engagement whenever a disaster incident needs to be opened. The initial actions are addressed to detect and assess damage inflicted by a disruption to nPlan. The notication sequence is listed below:

i. Based on the damage assessment, if nPlan will be unavailable to customers for more than 48 hours, the CEO will declare that a disaster has occurred and that the Disaster Recovery Plan has been activated. The CEO also has the discretion to activate the Disaster Recovery Plan based on other criteria.
ii. In the event customer data has been compromised, nPlan aims to notify its customers no later than seven days after the incident is reported.
iii. If the Disaster Recovery Plan has not been activated, the Recovery and Reconstitution phases will not be performed. Instead, The CEO and necessary team members will perform all appropriate tasks under nPlan's Incident Response Plan.

Service Level Agreement

1. Definitions

1.1 Target Service Uptime - Commencing at nPlan's activation of the Cloud Service, except during maintenance periods and force majeure events, nPlan targets a Cloud Service uptime ("Target Service Uptime") of 99.5%, calculated as (total time in preceding calendar month - Unplanned Downtime) ÷ total time in preceding calendar month, expressed as a percentage.

1.2 Unplanned Downtime - time during which the Client is unable to connect to the Cloud Service, with the exception of maintenance periods and force majeure events.

1.3 Service Credits - For any two months in a three month period in which the Target Service Uptime of the nPlan Cloud Service is below the applicable Target Service Uptime during a monthly reporting period, clients are eligible to receive "Service Credits" as a percentage of the affected monthly Cloud Services Fees:

- 5% when Target Service Uptime is less than 99.5% but greater than 99.0% in the applicable calendar month
- 10% when Target Service Uptime is less than 99.0%

2. Service Credits process

2.1 Should a client suspect that Target Service Uptime has not been achieved, it can request a calculation of the Target Service Uptime.

2.2 Clients are entitled to receive Service Credits if the Target Service Uptime of the affected Cloud Service is below the Target Service Uptime in any two months in a three month period. Claims for Service Credits must be made within sixty calendar days from the date the Service Credits became applicable.

2.3 Clients are entitled to receive only one amount of Service Credits per monthly reporting period in which the applicable Target Service Uptime is missed. The Service Credits will be provided only towards any outstanding balance for the Cloud Service that, as of the date the client receives the Service Credits, is owed to nPlan under the relevant order for such Cloud Services, and the provision of these Service Credits represents the client's exclusive remedy, and nPlan's entire liability, for the missed Target Service Uptime.

Version	Date	Detail	Author	Approved by
1.0	29/05/24	Initial version	Nick Williams	Alan Mosca
1.1	14/05/25	Reviewed and updated	George Oehlert	Alan Mosca