Overview apps and software applications of Nedap N.V. related to privacy

In the following overview you'll find per Nedap group a description concerning the various software applications and portals of:

- The purpose of the application/data processing;
- Which data therefor is used;
- The way the data is collected;
- Where this data is stored;
- If data is shared with third parties;
- Which retention periods are retained.

The collection, processing or usage of personal data derived from the following apps or web portals is based on the execution of the contract or is required for further optimization of our customer services as we monitor their usage of these services.

For the definition of personal information we kindly refer to our privacy statement and disclaimer.

Nedap Energy Systems

Apps

Nedap myPowerRouter (Android/iOS)
Purpose: Mobile application for myPowerRouter.com, intended as the interface for your PowerRouter on-the-go;
Data: No data is processed in this app. Only PowerRouter data is shown in the interface and therefore sometimes stored for caching purposes. For analyzing and monitoring error reports, only the use of the app itself is monitored without collection of personal data;
Method: Using the same credentials as for myPowerRouter.com, a client can log in to retrieve insight into the data of its PowerRouter;
Storage: Only locally on your mobile device, in the app, for caching purposes;
Third parties: None of your data is shared with third parties unless required otherwise by law;
Retention: Data is part of myPowerRouter.com, see its privacy policy for retention times.

If you have any questions after reading this document about protecting your privacy during your visit to our website or usage of the apps, please contact us via e-mail: support@powerrouter.com

Nedap Healthcare

Apps

Nedap Ons (Android/iOS)

The use of this app is only available and restricted to users with an account in Nedap ONS Administratie, without such account the app cannot be used for the purpose it is developed for.

Purpose: Sending of messages between colleagues and viewing of calendars out of Nedap ONS on a mobile device;

Data: Send and receive messages through ONS Berichten and calendar data from ONS Planning;

Method: The app doesn't collect any data of the mobile device. The app displays only data from the Nedap ONS Administratie SAAS application. For crash reports or analytical purpose only the use of the app is monitored without collection of personal data;

Storage: Calendar data will be stored encrypted on the mobile device. The sent and received messages are not stored on the mobile device. Crash data is stored encrypted on the mobile device;

Third parties: The app collects anonymous crash reports and analytical data about the use via third party service providers. None of the other data is shared with another system than Nedap ONS unless required otherwise by law;

Retention: Data of today and yesterday will remain in the application until the next connection with ONS Administratie. At the moment of connection this data will be updated.

Ons Toegangscode (Android/iOS)

The use of this app is only available and restricted to users with an account in Nedap ONS Administratie, without such account the app cannot be used for the purpose it is developed for.

Purpose: To facilitate a secure login procedure on ONS Medewerkerportaal;

Data: No data is processed in this app;

Method: The app doesn't collect any data of the mobile device. For crash reports or analytical purpose only the use of the app is monitored without collection of personal data;

Storage: No user data is stored in this app. Crash data is stored encrypted on the mobile device;

Third parties: The app collects anonymous crash reports and analytical data about the use via third party service providers;

Retention: No user data is stored in this app.

Ons Dossier (Android/iOS)

The use of this app is only available and restricted to users with an account in Nedap ONS Administratie, without such account the app cannot be used for the purpose it is developed for.

Purpose: Mobile access to clients file and editing reports;

Data: Client information, care plan and reports from ONS Administratie;

Method: The app doesn't collect any data of the mobile device. The app displays only data from the Nedap ONS Administratie SAAS application. For crash reports or analytical purpose only the use of the app is monitored without collection of personal data;

Storage: Crash data is stored encrypted on the mobile device;

Third parties: The app collects anonymous crash reports and analytical data about the use via third party service providers;

Retention: No user data is stored in this app.

Ons Medicatiecontrole (Android)
The use of this app is only available and restricted to users with an account in Nedap ONS Administratie, without such account the app cannot be used for the purpose it is developed for.
Purpose: Safely and quickly run duplicate checks when administering medication with increased risk.
Data: The double checks, including the attached photos taken with the camera on the mobile device, are added to the clients file in ONS Administratie;
Storage: Crash data is stored encrypted on the mobile device;
Third parties: The app collects anonymous crash reports and analytical data about the use via third party service providers;
Retention: No user data is stored in this app.

If you have any questions after reading this document about protecting your privacy during your visit to our website or usage of the apps, please contact us via e-mail: privacy-hc@nedap.com

Nedap Identification Systems

Apps

SENSIT Configurator App

- Purpose: Configuring and calibrating parking sensors, relay nodes, and gateways. The data is used to link the sensors in the SENSIT Interface Software;
- Data: User-configured parking sensors and GPS location of the sensor/node. This data is temporarily stored in a database (storage) until the user has sent this via e-mail or other "share" method. The data can be erased via a menu button. Required functionality / data smart device: location, storage, camera, account and Bluetooth;
- Method: Through communication over Bluetooth protocol with the Configuration Tool and use the GPS data from the phone or handheld;
- Storage: Database locally on the phone;
- Third party: Data is shared with the Nedap SENSIT Interface Software;
- Retention: The data is part of the operation and configuration of the SENSIT Interface Software. It will remain for the duration of the entire system.

P-License App

- Purpose: Identify parking permits at the parking spaces in the SENSIT system;
- Data: The P-License app detects the location of the user via GPS fix . By pressing the parking button, this location and license number is sent to the SENSIT server. Required functionality / data smart device: location, storage and camera;
- Method: The parking license QR code to be scanned using the camera by the user in the app. The location is determined by GPS;
- Storage: The parking permit is stored locally on the phone and on the Nedap SENSIT server, the GPS location is only stored on the Nedap SENSIT server;
- Third party: The information is shared with managers of the SENSIT system. They can see which parking permits are used at the parking location. Personal data of the user is not visible;
- Retention: The data is part of the operation and configuration of the SENSIT Interface Software. It will remain for the duration of the entire system.

P-Guide App

- **Purpose:** The P-guide app is part of the SENSIT platform, this can be used to navigate to a free parking spot;
- **Data:** For the correct operation of the P-Guide app, only access to location data and storage is required. When using the option 'permits', access to the camera is required, the camera is used to scan a QR code. Required functionality / data smart device: location, storage and camera;
- **Method:** When the P-Guide app is started, it is possible to monitor a particular parking for available spaces. In the background, the app keeps track of the monitored location and checks if the app is in the desired geo-fence location. Only within the geo-fence, the app sends the location of the app to the backend software. The transmitted data contains the location and a unique ID that is generated by the app only;
- **Storage:** The P-Guide app stores only news articles and images locally on the smart device, in a such way that the app can also be used offline. When using the "Permit" option, the permit is stored locally on the smart device;
- **Third Party:** Information will not be shared with third parties unless required otherwise by law;
- **Retention period:** Licenses are stored in the SENSIT Interface Software and are available during the lifetime of the system. Should a license be withdrawn, it will be erased permanently.

MACE App

- **Purpose:** The MACE app is a part of the MACE Platform, which makes it possible to use a smart phone as an identifier for an access control system;
- **Data:** For proper functioning, the MACE app requires the first name, last name, e-mail address and DeviceID. Required functionality / data smart device: location, storage, NFC, and Bluetooth. On Android devices, it is necessary to authorize the location data. Location information is not stored in the MACE Platform;
- **Method:** Virtual credentials are stored in the MACE app, they can be presented to a MACE reader via 'Near Frequency Communication (NFC), Bluetooth Low Energy (BLE) and QR codes. NFC and BLE are used by the MACE app to communicate with a MACE Reader;
- **Storage:** The virtual credentials are stored both locally on the phone and in the MACE Platform. The first name, last name, e-mail address and DeviceID are stored in the MACE Platform;
- **Third party:** The information from the Virtual Basic MACE UID is not shared with third parties. When using a MACE Virtual Credential, information is shared with the administrator and user of the relevant 'Company Space';
- **Retention period:** The data is part of the operation of the MACE Platform and will remain for the duration of the entire system. Nedap Identification Systems can permanently delete data.

Software applications / Portals

Business Partner Portal Nedapidentification (https://portal.nedapidentification.com)

- **Purpose:** The portal is used for offering commercial documentation, technical documentation and e-learning to Business Partners. For ICT logging purposes IP addresses of visitors can be stored;
- **Data:** In order to login into the portal, an e-mail address and password is required. Per user, the following information is stored: First name, last name, Name Business Partner, e-mail address, followed e-learning training, telephone number (optional) and date of user login;
- **Method:** User account details are entered using a web form;

- **Storage:** The data is stored within the EER;
- **Third party**: Data is not shared with third parties unless required otherwise by law. ;
- **Retention period: :** Account information will be available until the account is removed from the system. A user can send a removal request from within the application. The Nedap administrator receives a notification and the account will be removed from the system.

SENSIT SIS

- **Purpose:** Providing a management tool for issuing and managing Electronic Parking License (EPL) authorizations, and reporting potential parking violations. For ICT logging purposes IP addresses of visitors can be stored;
- **Data:** No personal data is stored within the SENSIT SIS application. If the Electronic Parking License option is applied, the first name, last name, license plate, EPL node ID, expiration date and exemption zone are recorded;
- **Method:**. Data is accessible through the Webinterface and a webservice;
- **Storage:** The data is stored in the SENSIT SIS application, all data is stored in a Private Cloud environment, owned and managed by Nedap located within the EER;
- **Third party:** The data is not shared with third parties without the permission of the responsible person unless required otherwise by law;
- **Retension period:** 'Electronic Parking Licenses' are stored in the SENSIT Interface Software, and are available throughout the system's running time. If a license is withdrawn, it will be permanently removed.

MOOV portal

- **Purpose:** For access to a closed area, it must be determined whether the concerned vehicle or person has rights to enter the area. For ICT logging purposes IP addresses of visitors can be stored;
- **Data:** The end user can decide which data to save in the application, but at least a name, identification number and template are saved. Further, all transactions of the VMC controllers are saved;
- **Method:** The authorization data is stored on the VMC controller, this involves the identification number and times of access. Transactions are sent in real time to the MOOV application, if it is not possible to send the transactions, they will be buffered on the VMC (FIFO max 100,000 events);
- **Storage:** All data stored in the MOOV application is in a Private Cloud environment, owned and managed by Nedap located within the EER;
- **Third party:** The data is not shared with third parties without the permission of the responsible person unless required otherwise by law;
- **Retension period:** The data is part of the operation of the MOOV application and will be preserved throughout the entire system. Nedap Identification Systems can permanently delete the data and also allows the transactions to be automatically deleted after an adjustable period.

MACE Portal

- **Purpose:** The MACE Portal allows you to manage credentials that allow you to use a smart device as a means of identification for an access control system. For ICT logging purposes IP addresses of visitors can be stored;

- **Data:** For the correct operation of the MACE app, a first name, last name, DeviceID and e-mail address are sufficient. Required smart device functionality / data: location, storage, NFC, and Bluetooth. With Android devices, it is necessary to give permission to the location data; Location data is not saved in the MACE Platform;
- **Method:** Virtual credentials are stored in the MACE app, they can be presented to a MACE reader via 'Near Frequency Communication (NFC), Bluetooth Low Energy (BLE) and QR codes. NFC and BLE are used by the MACE app to communicate with a MACE Reader;
- **Storage:** The virtual credentials are stored locally on the phone as well as in the MACE Platform. The first name, last name, DeviceID and e-mail address are stored in the MACE Platform located within the EER;
- **Third party:** By default, the information available in the portal is not shared with third parties without the permission of the responsible person unless required otherwise by law. When using a Virtual MACE Credential, the information is shared with the administrator and user of the respective 'Company Space';
- **Retension period:** The data are part of the operation of the MACE Platform and will be preserved throughout the entire system. Nedap Identification Systems can permanently delete the data.

If you have any questions after reading this document about protecting your privacy during your visit to our website or usage of the apps, please contact us via e-mail: privacy@nedapidentification.com

Nedap Library Solutions

Software applications / Portals

Business Partner Portal (www.nedaplibrary.com/support.html)

- **Purpose**: The portal is used for offering technical documentation and support to Business Partners. For ICT logging purposes IP addresses of visitors can be stored;
- **Data**: In order to login into the portal, an e-mail address and password is required;
- **Method**: User account details are entered using a web form. Per user, the following information is stored: Name Business Partner, e-mail address for support, financial and commercial contact,;
- **Storage**: Any data the user provides, are stored at Nedap secure servers or those of a third party within the EER or in the U.S. under the EU–US Privacy Shield. For the distribution of our newsletters we may use an US e-mail service provider (compliant with the EU-US Privacy Shield) and e-mail addresses may be processed in the US. For the processing of service-call tickets we may use an US service ticket provider (compliant with the EU-US Privacy Shield) and service calls may be processed in the US;
- **Third party**: We do not provide data to those other than the third parties who provide services to our website and partner portal, our chosen e-mail service provider and service ticket provider, unless required otherwise by law;
- **Retention**: The data will be stored till such time they change or are deleted by the user, or a request to remove the data from our database has been sent to us.

Librix Online portal (www.librixonline.com)

- Purpose: Used to identify users. For ICT logging purposes IP addresses of visitors can be stored;
- Data: User account information (username, e-mail address, date-time of last request and login, current and last login IP address). Per user, the following information is stored: Initials, First name, last name, e-mail address, telephone number;
- Method: User account details are entered using a web form, date-time stamps and IP addresses are gathered at login;
- Storage: The data is stored in the application database located within the EER;
- Third party: We do not provide data to third parties unless required otherwise by law;
- Retention The data will be stored till such time they change or are deleted by the user, or a request to remove the data from our database has been sent to us.

In case, after reading this document, you still have questions regarding the protection of your privacy while visiting our website(s) or using the apps, feel free to contact us via e-mail: info@nedaplibrary.com

Nedap Light Controls

Software applications / Portals

Luxon Live Server

- Purpose: the username and e-mail data is used for authenticating users who log in to the system. The (optional) telephone number is used in case a user needs to be contacted by the installation admin. For ICT logging purposes IP addresses of visitors can be stored;
- Data: every user needs to have its own account on the server. The required data for an account: username & e-mail address. A telephone number is optional;
- Method: the first installation admin account is created for the customer. After activating the account, using the unique link send to the e-mail address of the user, the user is able to update its personal data. Other users can be created by the installation admin by using a web form;
- Storage: username, e-mail address & telephone number are stored in the application database located within the EER;
- Third party: data is not shared with others unless required otherwise by law. The accounts created by an installation admin are visible for an installation admin within the same company;
- Retention: the data is kept in the system for as long as its associated account is active. Once an account is deleted, the associated data is also deleted.

Luxon Light Controller (LLC)

- Purpose: the first name, last name and username are used for authenticating users who log in to the system. For ICT logging purposes IP addresses of visitors can be stored;
- Data: every user needs to have its own account on the LLC. The required data for an account: first name, last name and username;
- Method: the first installation admin account is created for the customer. After login, the user is able to update its personal data. Other users can be created by the installation admin by using a web form;
- Storage: first name, last name & username are stored in the database that is on the unit itself on site;

- **Third party**: data is not shared with others unless required otherwise by law. The accounts created by an installation admin are visible for an installation admin within the same LLC;
- **Retention**: the data is kept in the system for as long as its associated account is active. Once an account is deleted, the associated data is also deleted.

Luxon Portal

- **Purpose**: Giving partners, end-users and staff access to product specifications, software, and commercial documentation. For ICT logging purposes IP addresses of visitors can be stored;
- **Data**: every user needs to have its own account on the portal. The required data for an account: user name and e-mail address;
- **Method**: users log in with their personal login data (user name and password);
- **Storage**: user name, e-mail address and login details are stored in the portal database within the EER. How regularly the user logs in and the last login time are also registered. This information is used for service purposes;
- **Third party**: data is not shared with others unless required otherwise by law;
- **Retention**: the data is kept in the system for as long as its associated account is active. Once an account is deleted at user's request the associated data is also deleted.

In case, after reading this document, you still have questions regarding the protection of your privacy while visiting our website(s) or using the apps, feel free to contact us via e-mail: privacy-lightcontrols@nedap.com

Nedap Livestock Management

Software applications / Portals

Nedap Livestock Management Newsletter (www.nedap-livestockmanagement.com/)

- **Purpose**: In order to send newsletters. For ICT logging purposes IP addresses of visitors can be stored;
- **Data**: E-mail address;
- **Method**: By using a web form;
- **Storage**: For the distribution of our newsletters we use an Australian e-mail service provider, the e-mail address is processed in Australia based on former user approval;
- **Third party**: Next to the external e-mail service provider data aren't shared with third parties unless required otherwise by law;
- **Retention**: Data will be available until the account is removed from the system. Receivers of the newsletter have the opportunity to unsubscribe. If they do, their e-mail address will be deleted from the database/list.

Business Insight

- **Purpose**: Used to identify the user and/or the farm inside the application. For ICT logging purposes IP addresses of visitors can be stored;
- **Data**: User account information (username, name, e-mail address) and/or farm information (name, address, zip code, city, telephone, e-mail, country);

- **Method**: User account details are entered using a web form. Farm information is received either by the Nedap Velos installation or entered by the user using a web form;
- **Storage**: The data is stored in the application database located within the EER;.
- **Third party**: Farm information can be shared (by user only) with other users within the application;
- **Retention**: Farm information is part of the operation/configuration of the Nedap Velos system. For that reason, data will not be removed from our system. User information is needed to identify the user. The user information will be available until we receive a removal request from the user.

Velos

- **Purpose**: Used to identify users. E-mail addresses are used to send notifications. For ICT logging purposes IP addresses of visitors can be stored;
- **Data**: This system contains account information (name, address, zip code, city, telephone number, e-mail address, language) of one or more users;
- **Method**: User account information is entered using the local on-site website;
- **Storage**: All data is stored in a database on the device (at the farm);
- **Third party**: Account information will not be shared with third parties unless required otherwise by law;
- **Retention**: Account information will be available until the account is removed from the on-site system.

Business Portal

- **Purpose**: Used to identify the user. Contact form is used to contact Nedap Livestock Management. E-mail address can be used to receive newsletters and/or activation links. For ICT logging purposes IP addresses of visitors can be stored;
- **Data**: Name, company, e-mail address, country, telephone number are required when using the contact form. Account information (first/last name, e-mail address, username, country, company, function) is required to create an account.
- **Method**: Information is entered by using a web form.
- **Storage**: Data is stored in a database located within the EER. For the distribution of our newsletters we may use an US
  e-mail service provider (compliant with the EU-US Privacy Shield) and e-mail addresses may be processed in the US;
- **Third party**: Account details aren't shared with third parties unless required otherwise by law. When using the newsletter the e-mail address of the user may be used by an external e-mail service provider;
- **Retention**: Account information will be available until the account is removed from the system. A user can send a removal request from within the application. The Nedap administrator receives a notification and the account will be removed from the system.

In case, after reading this document, you still have questions regarding the protection of your privacy while visiting our website(s) or using the apps, feel free to contact us via e-mail: privacy-livestockmanagement@nedap.com

Nedap Retail

Apps

Nedap Retail IdCloud App

- **Purpose**: Unlock the potential of RFID with !D Cloud. Count, program, print, search and destroy RFID labels using !D Cloud and gain full control over your inventory. Functionality of the smart device used: storage, camera, Bluetooth, Wifi;
- **Data**: Article data, expected stock and count information is locally stored on the smart device;
- **Method**: A RFID handheld reader is connected using Bluetooth to perform the operations needed. Bluetooth is also used to connect a barcode reader. The camera is used to read barcodes and to register the app using a QR code. Article and count information is transferred between !D Cloud and the smart device using network connection;
- **Storage**: A local article database is present on the smart device;
- **Third Party**: Data is not shared with third parties unless required otherwise by law;
- **Retention**: Data will be present on the device until the app gets a reset or will be removed.

Nedap Retail IdHand App

- **Purpose**: The app demonstrates the functionality of the Nedap Retail iDHand 2 RFID reader. Functionality of the smart device used: storage, Bluetooth;
- **Data**: RFID label information is retrieved from the labels;
- **Method**: A RFID handheld reader is connected using Bluetooth to perform the operation needed;
- **Storage**: RFID label information is stored in memory on the smart device;
- **Third Party**: Data is not shared with third parties unless required otherwise by law;
- **Retention**: Data will be present on the device until the app is closed.

Nedap Retail Analytics App

- **Purpose**: The Nedap Retail Analytics app shows you everything that is happening in your stores, regarding loss prevention, store performance and stock management. This across countries and regions. You can take direct action to ensure optimally controlling operational costs and improving the security level of your stores. Functionality of the smart device used: storage, camera, Wifi;
- **Data**: Data is retrieved from Nedap Retail Analytics and shown in the app;
- **Method**: The app uses the camera to register the app via a QR code. Wifi is used to communicate to Nedap Retail Analytics;
- **Storage**: Analytics information is stored locally on the smart device;
- **Third Party**: Data is not shared with third parties unless required otherwise by law;
- **Retention**: Data will be present on the device until the app is removed or gets a reset.

Software applications / Portals

Nedap Retail Customer Portals:

Nedap Retail Analytics (https://nedapretailanalytics.com)
Nedap Retail !D Cloud (https://idcloud.nedapretail.com)
Nedap Retail Cube (https://cube.nedapretail.com)
Nedap Retail Device Management (https://devices.nedapretail.com)
Nedap Retail Easinet (https://www.nedapretail.com/wwwroot)

- **Purpose**: Used to identify the users of the portal. For ICT logging purposes IP addresses with date-time stamp of visitors are stored;
- **Data**: Account information (user name or alias and e-mail address). Date-time stamps and IP addresses.
- **Method**: Account details are entered using the 'Device Management Portal'. Date-time stamps and IP addresses are gathered at login;
- **Storage**: The data is stored in the application database located within the EER;
- **Third Party**: We do not provide data to third parties unless required otherwise by law;
- **Retention**: The data will be stored till such time they change or are deleted by the user, or a request to remove the data from our database has been sent to us.

Nedap Retail Partner Portal (https://portal.nedapretail.com)

- **Purpose**: Used to identify the user in order to determine if access to the partner portal is justified and contact details
  for sending requested product information, documentation and software. For ICT logging purposes IP addresses of visitors can be stored;
- **Data**: Account information (user name, business e-mail address, business telephone number);
- **Method**: Account details are entered using the application;
- **Storage**: The data is stored in the application database located within the EER. For the distribution of our newsletters we may use an US e-mail service provider (compliant with the EU-US Privacy Shield) and e-mail addresses may be processed in the US;
- **Third Party**: We do not provide data to those other than the third parties who provide services to our partner portal and
  our chosen e-mail service provider, unless required otherwise by law;
- **Retention**: Any data users provide us with will be stored till such time they change or delete their account, or request us
  to remove their data from our database or till the cooperation between the partner and Nedap Retail is terminated

Nedap Retail Commercial Websites (www.nedap-retail.com, www.nedap-idcloud.com)

- **Purpose**: Used to revert back to the users contact request. For ICT logging purposes IP addresses of visitors can be stored;
- **Data**: User information (user name, title, business e-mail address, business telephone number);
- **Method**: User details are entered using a web form;
- **Storage**: The data is stored in the application database located within the EER. For the distribution of our marketing information we may use an US e-mail service provider and/or marketing information provider (compliant with the EU-US Privacy Shield) and entered data may be processed in the US;
- **Third Party**: We do not provide data to those other than the third parties who provide services to our website, our chosen e-mail service provider and marketing information provider (compliant with the EU-US Privacy Shield), unless required otherwise by law.
- **Retention**: Any data users provide us with will be stored till such time they change or are deleted, or a request to remove the data from our database has been sent to us.

In case, after reading this document, you still have questions regarding the protection of your privacy while visiting our website(s) or using the apps, feel free to contact us via e-mail: privacy-retail@nedap.com

Nedap Security Management

Software applications / Portals

Nedap Security Management website and partner portal

- Purpose: Used to identify the user in order to determine if access to the partner portal is justified and contact details for sending requested product information, documentation and software. For ICT logging purposes IP addresses of visitors can be stored;
- Data: Name, company name, address, business e-mail, telephone number and country;
- Method: Account information is entered using the application;
- Storage: Any data the user provides, is stored at secure servers or those of a third party within the EER. For the distribution of our newsletters we may use an US e-mail service provider (compliant with the EU-US Privacy Shield) and e-mail addresses may be processed in the US.;
- Third party: We do not provide data to those other than the third parties who provide services to our website and partner portal and our chosen e-mail service provider, unless required otherwise by law;
- Retention: Any data users provide us with will be stored till such time they change or delete their account, or request us to remove their data from our database or till the cooperation between the channel partner and Nedap Security Management is terminated.

In case, after reading this document, you still have questions regarding the protection of your privacy while visiting our website(s) or using the apps, feel free to contact us via e-mail: info@nedapsecurity.com

The above information might change due to developments in the market and/or products and we kindly request you to regular consult this page.