DNA's data protection statement

Data protection has always been a key part of our operations, and the protection of personal data and privacy is of paramount importance to us. We process personal and communication data on a daily basis and want to be worthy of the trust of our customers. We comply with the legislation in force in Finland and the guidelines issued by the authorities.

DNA processes personal data for a variety of reasons. In this statement, we explain how we process the personal data of current and potential customers, users of services, invoice payers, participants in sweepstakes, contests and opinion and market surveys, those contacting our customer service, business contacts, employees of our corporate customers, responsible persons and persons with authorisation to sign.

In this data protection statement, we explain e.g. the following:

- the practices we use at DNA to ensure the privacy and confidentiality of communications of our customers, users of our services and other data subjects;
- what personal and other data we collect,
- how and on what basis we process this data,
- what affects the retention period of data and to whom DNA may disclose personal data, and
- the rights of the data subject.

The data protection policy does not apply to services or websites provided by other companies, even if access to these services is through DNA's services.

Why is personal data collected?

We use personal data primarily for the technical implementation of our services and for managing the customer relationship, such as invoicing. We also collect data to improve customer experience and further enhance our services. At the same time, we also target services to meet the individual preferences of our customers and service users.

For what purposes is data collected and on what legal basis?

For the performance of contracts, the provision and production of services

We use personal data primarily for the performance of contracts, the transmission of communications, the provision and production of services. This data allows us to verify personal data and verify credit information before making an offer and concluding a contract, to provide and manage services ordered and provided by the contract, to develop services and the offering, to correct failures and incidents, to ensure the security of services, and to improve user experience.

In addition to managing the customer relationship, the data is also used for invoicing, monitoring and recovering receivables, and preventing and investigating possible abuses and frauds. We also process data for customer service and customer communications, for example, to send service notifications and to communicate concerning our services.

We process communications data for the development of communication services and the communication network. Personal data is also processed for the purpose of targeting and personalising service content and making recommendations which, based on the collected data, we consider to be appropriate and interesting for users of the services. In addition, the data is used to develop, test and control the quality of processes and systems, and to analyse and keep statistics on the use of products and services. We process data to better understand the needs of service users, we may group data, e.g. using usage groups, quantities and invoicing, and to find out, for example, how different user groups use the services. Personal data may also be processed for marketing measures included in the service or contract.

On the basis of a legitimate interest

We use both group-level usage data and person-related data for direct advertising, distance selling, addressed transmissions, as well as other marketing, market and opinion surveys of DNA and its affiliates and DNA's partners. We also process personal data provided to us concerning direct marketing bans. In the case of contact persons and decision-makers of corporate customers, DNA can send electronic direct marketing on the basis of DNA's legitimate interest. The recipient of marketing may at any time prohibit the marketing through the link in the email or through DNA's corporate customer service.

Personal data is also processed based on the legitimate interest of DNA to prevent and investigate possible abuses and frauds.

Legal obligations

We process data for the purpose of performing obligations under law and authority decisions, including for the following purposes: accounting, the prevention, detection and investigation of money laundering and fraud, obligations relating to payment services, and coercive measures under police and coercive legislation. The data may also be disclosed in accordance with the requirements set by the competent authority and legislation.

On the basis of consent

You can give your consent to electronic direct marketing. If your data is processed on the basis of consent, you also have the right to withdraw your consent. You can manage your marketing authorisations in DNA's online My Services or by contacting DNA's customer service. In the case of contact persons and decision-makers of corporate customers, DNA can send electronic direct marketing on the basis of DNA's legitimate interest and also on the basis of the person's consent. The recipient of marketing may at any time withdraw their consent or prohibit the marketing through the link in the email or through DNA's corporate customer service.

When DNA is the administrator of a page on Facebook, Facebook and DNA are joint controllers. We collect data on, for example, the insights from DNA's Facebook pages and the visibility of posts. For more information about the processing of personal data, please see Facebook's Data Policy.

What are the benefits of collecting data for the data subject?

We use data primarily for the provision, maintenance and analytics of services. We use this data to improve our product range, make services more functional, ensure invoicing accuracy, maintain information security and prevent misuse of services.

We also use the data to improve customer experience and to make DNA‘s services more personal, user-friendly and interactive, for example, a DNA service or the dna.fi website may use the data to recommend content or products that are likely to be of interest to the user. Recommendations are based on the fact that the data can be used by the service or website to predict what kind of products or content the user wants to view. We may also use the data for market research and customer satisfaction surveys.

For marketing, we aim to target offers and other advertising to make them as interesting and relevant as possible to the user. When the user is e.g. logged into our website, we may show them an offer that we have considered interesting and relevant to them based on the services they have used or tried or have already ordered. For example, based on the phone model used by the customer, they can receive a targeted ad of a new device or a type of subscription that best suits the characteristics of the device. Targeting can be done in DNA-managed services and channels (e.g. dna.fi) as well as on websites and services that sell advertising space.

Automated decision-making

When concluding a contract, DNA has the right to verify the customer's credit history in order to implement the contract. Automated decision-making may be used in the credit information verification. You can request a manual decision-making process instead of automated, provide further clarification or challenge a decision based solely on automated processing.

What data does DNA collect and how?

Personal data is collected by us in many different ways. For example, data is stored in connection with contracts, competitions, campaigns or surveys. DNA can also examine customer satisfaction regarding the service the customers received by sending a customer satisfaction survey by, for example, a text message or email, by calling or conducting a study or survey online. Personal data is also stored when a service is deployed and registered for, when services are used, when a person communicates with our customer service, visits DNA's website or subscribes to DNA's newsletter.

What personal data is collected?

When entering into a contract or registering for a service, we collect as personal data the customer's basic information such as name, personal identity code, address, telephone number, email address, language information, identification information and customer ID information. If the service has a separate user or invoice payer, we collect their name and contact details, and for the user, their personal identity code or date of birth may also be collected. For corporate customers, we collect the name, contact, role and position information of the company's contacts and users, and the personal identity code of the person with authorisation to sign for the company.

Other data collected and processed in relation to the contractual relationship, service use and contact history may include: services, products and devices ordered and their value and warranty time, start and end dates of contractual relationships, opening and closing dates of services, order and delivery dates, times of service use, cancellation and refund information, registrations with any bonus agreements, user IDs, SIM card numbers, IMEI codes or other identifiers of devices, service use and availability addresses, service changes, and bans on the publication of list information. In addition, we collect data about customer communications, customer feedback, responses to customer satisfaction studies and surveys and interest in products or services, and marketing authorisations and bans. In addition, data related to invoicing, payment and collection (e.g. invoicing method, invoicing contact details) is processed and in connection with the conclusion of contracts, the customer's credit information from the check date may be

processed. We also collect information on the device in use when the customer inserts the SIM card into the device and opens it. We also collect information from the person themselves in different channels.

When using DNA's network and communication services, traffic data is stored in systems when a message is transmitted, including data about the parties to calls and messages and the duration and time of calls. Data is also stored about location, connection routing and data transfer protocols. When using DNA's broadband services, for example, data attached to the user is stored, including IP address, device operating system, session ID, session time and duration and data collection channel (internet browser, mobile browser and browser version). We process traffic data for the implementation, development, invoicing and troubleshooting of the communication service, as well as to resolve abuses and ensure information security. Traffic data may also be processed with the customer's consent for marketing purposes. In connection with the WiFi Network Optimisation Service, DNA can update the software and settings of the modem connected to the network, if necessary. Data collected in connection with the service includes the model and software version of the modem, name of the WiFi network, connected devices and the amount of data transferred on the devices. The data is processed to provide and develop the service as well as to investigate potential error situations and problems. Data created and processed in connection with the service is stored for the abovementioned purposes for 30 days. Anonymised data might be stored for longer.

When using other than communication services, data is accumulated about the use and communications of service and content usage, such as usage, search and browsing data for service features. For DNA's TV services, for example, the following data are stored: date and time of use, which content is viewed through DNA's TV service, device data, operating system, language selection, and information on network and device performance. DNA TV's data protection statement can be found here.

A randomly generated number sequence, which can be linked to a cookie, is created for a registered user identified through DNA's online services or for a person who has opened an email sent by DNA. An unregistered user is identified by a cookie. You can read our cookie policy here. When the user navigates to the DNA.fi website via a link (e.g. through a search engine results page), not only the browsing history of the service is stored, but also data about the website from which the DNA website was accessed.

Customer service and sales calls for consumer and corporate customers are recorded, and chats, emails or text messages between DNA and those who contact DNA are stored. Recorded or otherwise stored communications and call recordings can be used to verify business and customer service transactions and contracts that have been created and to resolve complaints and unclear situations. In addition, recordings are used for training related to customer service and other customer interfaces, developing service and operations, surveying customer opinions and monitoring quality in marketing targeting and personalisation. Recordings can also be used to detect possible abuses and to ensure security. The recordings will be destroyed when they are no longer required for the above-mentioned purposes.

In DNA Store premises, camera surveillance can be used to ensure the safety of those present on the premises, to protect property and to prevent or resolve situations that endanger safety and property.

In our marketing register, we store personal data, including name, occupation, age/year of birth, mother tongue, gender, contact details, preferred forms of communication, direct marketing authorisation and ban information and data on changes made to these data, also the person's role and position in the company and professional interests may be stored.

From which sources is data collected?

We collect personal data, other customer data and data describing service use in connection with the conclusion of contracts, service registration, competitions, campaigns, surveys, customer satisfaction surveys, sales and marketing events and customer service communications and service deployment and use, or otherwise from data subjects themselves.

We collect personal data about the use of our services, communication network and the dna.fi website.

Personal data may be collected and updated from public sources, such as corporate websites, the Finnish Trade Register, Population Register, Post, Intellia Oy, Fonecta Oy, the ban register maintained by Data & Marketing Association of Finland, public registers of authorities (e.g. business registers) and other similar third-party registers. When using the network, our systems also accumulate operator-related traffic data about phone calls, messages and location.

What rights does the data subject have?

Data subjects may exercise the rights listed below by contacting our customer service. The request must be sufficiently specified. Requests are assessed on a case-by-case basis, and DNA must verify the identity of the data subject before carrying out the request. We will inform you if we cannot fulfil the request in all respects, such as erase data that we have a statutory obligation to store.

Right of access

Data subjects have the right to access and review their personal data stored by us or verify that we do not store any of their personal data. In most cases, this data can already be seen in our My Services online service. The right of access may be restricted, for example, by virtue of legislation, privacy of other persons and DNA's business secrets. More information on access to your personal data can be found here.

Right to rectify inaccurate or incomplete data

If the data we store are inaccurate or incomplete, the data subject has the right to request their rectification.

Right to erasure

The erasure of data may be requested, provided that

- the data are no longer required for their specified purpose,
- there are no longer legal grounds for their processing.
- the data have been processed on the basis of consent and the data subject withdraws their consent or objects to the processing of the data, and there are no other justified grounds for the processing.

Please note that personal data which are necessary for the implementation of their purposes (e.g. if you have imposed a marketing ban, we retain the information on the ban and the contact details so that we can ensure compliance with the ban) or needed, for example, for invoicing or accounting purposes or other legal obligations, cannot be erased. It should also be noted that an erasure at the data subject's request is irrevocable, and we cannot recover data that has already been erased.

Right to restrict the processing of data

Data subjects may request that we restrict the processing of their personal data if they contest the accuracy of the data and the lawfulness of processing. A request for a restriction means that the processing of data is restricted in order to retain it until the accuracy of the data is verified.

Data subjects have the right to object to processing by DNA for purposes of targeted marketing and direct marketing. In this case, the data subject's details are added to DNA's register for opting out of marketing.

For some services or campaigns, the terms of the contract or campaign may be accompanied by an electronic permission for direct marketing. In these cases, the processing of personal data for marketing may also be objected to.

Please note that in the event that a data subject has objected to processing for marketing purposes, DNA may still send messages related to the maintenance of the customer relationship and services, such as announcements on changes to contracts and service disruptions.

Right to object to processing

Data subjects have the right to object to processing by DNA for purposes of targeted marketing and direct marketing. In this case, the data subject's details are added to DNA's register for opting out of marketing.

For some services or campaigns, the terms of the contract or campaign may be accompanied by an electronic permission for direct marketing. In these cases, the processing of personal data for marketing may also be objected to.

Please note that in the event that a data subject has objected to processing for marketing purposes, DNA may still send messages related to the maintenance of the customer relationship and services, such as announcements on changes to contracts and service disruptions.

Right to transfer data

The data subject may request the transfer of data provided by themselves in a machine-readable format. This right applies only to personal data which have been processed automatically and on the basis of consent or the performance of a contract. As a result, the content of the data may be narrower than DNA's response to the right of access request. The file is delivered in csv format.

Transfers and disclosures of personal data and criteria for determining retention period

Our personnel and subcontractors are bound by professional secrecy and are prohibited from using confidential information. Personal and traffic data are processed only by those designated DNA employees or individuals working on behalf of DNA who are required to do so for the performance of their duties. Persons who have been entitled to process the data may do so only to the extent necessary for the performance of individual tasks.

Who at DNA processes customer data, is data disclosed or transferred?

DNA is part of Telenor Group and data is processed only by those employees of the group who are required to do so for the performance of their duties. Personal data may be processed, disclosed and transferred between Telenor Group companies for the purposes described in this statement and, for example, for reporting purposes and to use centralised information systems.

We use subcontractors and partners for data processing, service production and provision. A part of the data can be stored by DNA's subcontractors and partners due to reasons related to the technical or operative implementation of data processing, and data may also be otherwise processed through technical interfaces.

As a rule, we process data within the European Union (EU) and the European Economic Area (EEA). When we use subcontractors and partners, we ensure an adequate level of protection and careful and proper processing of the data as required by law through contractual arrangements and in an appropriate manner. Data may also be transferred outside the EU and the EEA. In this case, we will use data transfer mechanisms adopted by the European Commission, such as standard contractual clauses adopted by the European Commission.

DNA has an obligation to disclose information about our customers and service users to the authority requesting the information, to the extent laid down by law, e.g. to Finnish Transport and Communications Agency, the Data Protection Ombudsman, the police, the emergency services and other authorities on legal grounds or based on the decision of the competent authority.

In the event of copyright infringement, DNA is obliged to disclose personal data relating to IP addresses to the applicant or their representative registered on the basis of a decision issued by the Market Court pursuant to Section 60a of the Finnish Copyright Act.

To contact services. DNA may disclose contact information about the customer's or user's name, address and telephone number for publication in the subscriber list and number service, unless such publication is prohibited. DNA will disclose the contact information to Suomen Numeropalvelu Oy, through which contact information is available in services, including: Directory enquiry 118, Fonecta 020202, electronic directory services (Fonecta and Eniro). DNA is also obliged to disclose data declared for publication in the list to other providers of directory services.

It is possible to ban the registration and disclosure of personal data in whole or in part to the contact service. The subscription number that is the subject of the ban is called a secret number. A secret number must be separately agreed with us. DNA will delete and correct any incorrect data on request in an appropriate manner. However, it should be noted that an error in the paper list can only be corrected or removed when the following list appears.

Data is disclosed to other telecommunications companies or service providers that offer or provide services, e.g. for invoicing and in case of incidents and disruptions. Telecommunications companies exchange data on the use of communication and other services for the invoicing of services. For example, when you use roaming services provided by other operators (e.g. when travelling abroad), these operators have the right to obtain data from DNA and to collect and process your personal data.

Data may be transferred to designated partners performing DNA marketing for the purpose of targeting advertising, as well as for conducting opinion and marketing surveys. Media, advertising networks and online services can target DNA's advertising based on behavioural data collected from DNA's website, such as the page downloads made by the customer on dna.fi pages and the interest profile data that is connected to the browser.

DNA may also disclose data to a third party in order to protect or defend legal claims, DNA or its employees' interests, or to resolve crimes, collect receivables and investigate any violations. if we were involved in a company or business transaction, we may also disclose data to parties involved in the transaction and their advisors.

What is the retention period for personal data or the criteria for determining the retention period?

The retention period varies depending on the data and how long it is needed for the intended purpose, or for as long as required by law and regulations.

We retain personal data relating to the contractual relationship, use and registration of services, contact history and investigations for at least 3 years after the end of the customer and contractual relationship or the termination or last login of a registered service, for reasons such as consumer trade obligations, warranty obligations, receivables collection and any invoice complaints.

Data on the use of the dna.fi website is retained for at least 14 months. Personal data of participants in competitions and sweepstakes are retained for the duration of competitions and sweepstakes and until the winner has been contacted. Personal data stored in the marketing register and marketing ban register is retained for an indefinite period.

The legislation also obliges the storage of personal data, for example the Finnish Accounting Act requires the retention of accounting documents for a period of 6 years. We must also retain certain communications-related data for authorities for use in criminal investigations. For this purpose, for example, mobile network call and SMS traffic data must be stored for 12 months and IP addresses for 9 months from the communication transaction. In connection with the prevention and detection of money laundering, identification data on payment services must be retained for 5 years after the termination of the contractual relationship.

The retention period for recordings of corporate customer service and sales calls is 24 months. The retention period for recordings of consumer customer service and sales calls is 27 months. Recordings are needed to verify business and service transactions for fixed-term contract periods. If the data subject wishes to check their data in relation to call recordings, in addition to the personal data of the data subject, the data subject must specify the subscription number which has been used to call DNA's customer or sales service or which DNA has called, and the time of the call. For security reasons, the recording is usually delivered in written form.

Camera surveillance recordings are stored for 60 days. For security reasons, DNA does not disclose camera surveillance data to the data subject, but any checking of the recording will be carried out at a predetermined time in a DNA Store location. If the data subject wishes to check the camera surveillance recording concerning them, they must specify, in addition to their personal data (including picture), data of the DNA Store location, the date and time of the transaction. The right of access applies only to the images of the recording in which the data subject is present. The right of access to a recording may be restricted due to the privacy of other persons.

How is data protection and privacy ensured?

We value the privacy of all data subjects. DNA provides services in an industry where information systems and data protection are an integral part of our operations. For this reason, we ensure that our information security is always at a high level. Personal data is processed only by designated employees bound by professional secrecy. Data is always processed confidentially.

How does DNA ensure the security of services?

As the privacy of data subjects is of paramount importance to us, we ensure the effective protection of personal and traffic data and employ the necessary technical and administrative security measures to protect the data from unauthorised access, destruction, disclosure or other unlawful processing.

Our personnel are bound by professional secrecy. DNA personnel processing personal and identification data and individuals who process said data on behalf of DNA are bound by professional secrecy on data they process as part of their duties. The processing of personal data is a part of the orientation for new employees, and all employees receive periodic training on data protection matters. All employees are bound by an obligation of professional secrecy under law or as agreed and documented separately in individual employment contracts.

Management of access rights. DNA employs a system for managing the granting of access rights and the monitoring of their use. Personal data and other customer data are processed only by those designated DNA employees or individuals working on behalf of DNA who are required to do so for the performance of their duties. Personal data and customer data are disclosed to requesting authorities or rightsholders only in the event that said authority or rightsholder is legally entitled to the data.

Security of services. DNA ensures the information security of its services by applying various procedures in appropriate relation to the severity of the threats, the technical development level and costs. The data is saved in databases that are protected by firewalls and other technical means. The databases are located in locked and guarded premises, and the data can only be accessed by predefined and designated persons. Administration connections to servers and purchase events and the transfer of customer data in connection with invoicing material are implemented using secure connections. In order to prevent security breaches and to eliminate data security incidents, DNA may take the necessary steps, e.g. by removing viruses and malware from messages, preventing email messages from being received, and taking other similar and necessary technical measures. We aim not to unnecessarily compromise the confidentiality or privacy of the message when performing the above measures.

The responsibility of the service user for security. The customer and service user also have a responsibility for adequate security, e.g. by using devices in a careful manner and monitoring their use, and ensuring that up-to-date antivirus and firewall services and operating systems are used. If the customer uses PIN codes, passwords or other special identifiers when using services, the customer is responsible for the protection of such information.

Information on security-related issues. DNA will provide information on procedures related to the data security of the service and other factors related to data security in an appropriate manner and whenever possible on a website or by using customer bulletins, for example.

What can be seen from message traffic?

DNA processes all data generated from message traffic confidentially. When using DNA's network, our systems also accumulate traffic data about phone calls, messages and location. The traffic data can show, among other things, the time of calls and messages, the parties, how long the call lasted, and the location information. Data is also stored about location, connection routing and data transfer protocols.

DNA processes communications traffic and location data in accordance with the Act on Electronic Communications Services for the purpose of providing services, invoicing, technical development (such as optimising the operation of communications networks), detecting abuses or ensuring security.

Data may also be processed for the invoicing of other telecommunications companies and service providers, in cases of abuse and troubleshooting, and to ensure security. With consent, data may also be processed for marketing purposes.

How is location data processed and what is it used for?

Location data indicates the geographical location of the mobile phone and is used to provide location services and technical assistance for the transmission of communications. The accuracy of location data can vary considerably depending on the location of base stations. Significant differences can arise between urban areas and sparsely populated areas.

Location data can be used in many services, for example when the user orders information on a mobile phone about the location of the nearest pharmacy or flower shop, or when displaying location-based weather information or news. Locating requires the prior consent of the locatee.

Location data includes the address of the base station through which the service (for example, phone call or text message) is transmitted to your subscription. The accuracy of the provided location data can vary considerably depending on the location of base stations.

How is the privacy of children taken care of?

Our customers must be of legal age, so it is important that the customer also informs us of a minor using the subscription by registering them as a user of the subscription.

In the case of a subscription user under the age of 15, their guardian is entitled to receive a breakdown of the subscription invoice, specifying the subscription numbers of the parties to the communication or other full identification data, or the traffic data indicating the location of the device.

Contact

Data controller: DNA Plc, Business ID: 0592509-6, P.O. Box 10, FI-01044 DNA (street address Läkkisepäntie 21, FI-00620 Helsinki)

DNA Plc (on its own behalf and on behalf of its subsidiaries) is responsible for the processing of the personal data it collects. DNA has also appointed a Data Protection Officer. You can also contact DNA's Data Protection Officer through the address above. If you have any questions about the data protection statement or the processing of your personal data or you wish to exercise your rights under data protection legislation, contact us by mail at the above address or by email at palvelu@dna.fi.

For instructions on how to make an access request, visit the “If you want to know what data is collected about you, how to proceed?" section under Explore data protection . Please note that we ask you to verify your identity before we can act on your request or complaint. We may also ask you for more information to target your request to the correct register.

If you are not satisfied with the answers you receive, you can also contact the data protection authority.