NetSupport DNA and GDPR Compliance

Introduction

The ***EU General Data Protection Regulation ("GDPR")*** comes into force across the European Union on 25th May 2018 and brings with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age.

NetSupport DNA is a suite of easy-to-use tools for managing and supporting IT assets across a school network or campus. Its features include automatic discovery of devices; hardware and software inventory; change tracking and software licence management; energy monitoring; power management; USB endpoint security; printer monitoring; application and internet metering; a flexible alerting suite; and an easy-to-use software distribution module. NetSupport DNA also supports eSafety and safeguarding with keyword and phrase monitoring to alert schools of any online activity that may place a student at risk; internet monitoring of websites visited; the option for students to report concerns directly to trusted staff; and more.

The NetSupport DNA product does store and process personal data and, as such, is impacted by GDPR. The aim of this document is to provide you with all the information you need relating to the NetSupport DNA product to ensure that personal data is processed in accordance with these new regulations.

How does NetSupport DNA process Personal Data?

NetSupport DNA uses an agent installed on computers to gather inventory, usage and safeguarding data. The NetSupport DNA Agent will record the following information:

Hardware Inventory

The details of which Hardware inventory details are recorded are not relevant to GDPR as these are not considered personal data and therefore will not be listed in this document.

Software Inventory

As with hardware inventory, the software inventory is not classed as personal data and is therefore not detailed in this document.

Usage Information

The following usage information may be recorded

- All log on, log off, lock and unlock events
- All power on, power off events
- All applications started and closed
- All websites visited
- All print jobs set to printers

Safeguarding Information:
When the DNA agent matches one of the configured safeguarding phrases, the following information may be recorded:

- The phrase that was matched and the context it was used in (if the work was typed).
- A picture taken from the webcam, if present.
- A screenshot of the screen at the time the phrase was matched.
- A video showing the computer screen before and after the phase was matched.
- If the Device has a webcam, then this can be configured to take an image of the person using the computer.

All this information is recorded at the Agent machine, sent to the NetSupport DNA Server (using a proprietary communications protocol) and is then processed and stored in the NetSupport DNA database.

Where is the Personal Data stored?

NetSupport DNA is an on-premise solution and runs on servers located at the school. The data stored in NetSupport DNA is stored in an SQL server database that is either installed as part of the installation or a pre-existing SQL database server. Where sensitive data is stored in the NetSupport DNA database, this data is stored in an encrypted format. Where the SQL database server is installed as part of the NetSupport DNA installation, any direct access to the database is restricted by the security policies built into Microsoft SQL Server 2012. Where a pre-existing SQL server is used, the access is controlled by the security policy in place for the pre-existing SQL server.

If DNA Cloud support is enabled, then some of the personal data stored in the on-premise SQL Server databases is replicated to the NetSupport Cloud. All data replicated to the NetSupport Cloud is sent using SSL and is also encrypted by the DNA Server before being transmitted.

The NetSupport Cloud is hosted on Microsoft Azure in the UK's southern region. For information on the physical security of the Microsoft Azure Datacentre, please see:
https://docs.microsoft.com/en-GB/azure/security/azure-physical-security

What Data is collected and stored?

The table below lists all of the personal information that is stored in the on-premise NetSupport DNA database.

Name	Purpose	Legal Grounds	Sensitivity	Collection
Name	Identification	Legitimate interests	Personal Data	Automatically collected
Logon Name	Identification	Legitimate interests	Personal Data	Automatically collected
Email Address	Communication	Legitimate interests	Personal Data	Optional Data
Phone Number	Communication	Other	Personal Data	Optional Data
Mobile Phone Number	Communication	Other	Personal Data	Optional Data
Pager Number	Communication	Other	Personal Data	Optional Data
Department	Identification	Other	Personal Data	Optional Data
Employee/Student No	Identification	Other	Personal Data	Optional Data

Address	Communication	Other	Personal Data	Optional Data
City/Town	Communication	Other	Personal Data	Optional Data
County/State	Communication	Other	Personal Data	Optional Data
Post/Zip Code	Communication	Other	Personal Data	Optional Data
Typed Phrases	Safeguarding	Legitimate interests	Sensitive Data	Automatically collected
Screen Capture	Safeguarding	Legitimate interests	Sensitive Data	Automatically collected
Webcam Image	Safeguarding	Legitimate interests	Sensitive Data	Automatically collected
Accessed URL	Safeguarding	Legitimate interests	Personal Data	Automatically collected
Title of Accessed URL	Safeguarding	Legitimate interests	Personal Data	Automatically collected

If DNA Cloud support is enabled, the following data is also stored in the DNA Cloud:

Name	Purpose	Legal Grounds	Sensitivity	Collection
Name	Identification	Legitimate interests	Personal Data	Automatically collected
Logon Name	Identification	Legitimate interests	Personal Data	Automatically collected
Email Address	Communication	Legitimate interests	Personal Data	Optional Data
Phone Number	Communication	Other	Personal Data	Optional Data
Mobile Phone Number	Communication	Other	Personal Data	Optional Data
Pager Number	Communication	Other	Personal Data	Optional Data
Department	Identification	Other	Personal Data	Optional Data
Employee/Student No	Identification	Other	Personal Data	Optional Data
Address	Communication	Other	Personal Data	Optional Data
City/Town	Communication	Other	Personal Data	Optional Data
County/State	Communication	Other	Personal Data	Optional Data
Post/Zip Code	Communication	Other	Personal Data	Optional Data
Typed Phrases	Safeguarding	Legitimate interests	Sensitive Data	Automatically collected
Screen Capture	Safeguarding	Legitimate interests	Sensitive Data	Automatically collected
Accessed URL	Safeguarding	Legitimate interests	Personal Data	Automatically collected
Title of Accessed URL	Safeguarding	Legitimate interests	Personal Data	Automatically collected

NetSupport DNA and the GDPR data subject rights

The GDPR defines eight rights of the individual with regard to the processing of personal data. Part of complying with the new regulations is to ensure that you can comply with these individual rights. In this section, we explain each right and how it affects the NetSupport DNA product.

The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. For further information and guidance see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

NetSupport DNA has an “Acceptable Use Policy” feature and we recommend that as part of your acceptable use policy, you should either notify users that they are being monitored and what data is being recorded, or direct them to your privacy policy that should contain this information.

The right of access

Under GDPR, individuals have the right to access their personal data. This allows individuals to be aware of and verify the lawfulness of the processing.

See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

With a data subject access request, NetSupport DNA provides an export facility in the database maintenance tool that can be used to export the required data.

The right to rectification

Under Article 16 of the GDPR, individuals have the right to have inaccurate personal data rectified. See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/

The NetSupport DNA Agent installed on all computers has a feature available so that any user can view and update their personal information. Alternatively, this information can be updated manually by using the NetSupport DNA Console application.

The right to erasure

Under Article 17 of the GDPR, individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances. For information on when this right is applicable, see the ICO guidance at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

If this is applicable, then using the Database Maintenance feature from the NetSupport DNA Console, you can delete all the information related to an individual.

The right to restrict processing

Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. The right is not absolute and only applies in certain circumstances. In most cases, you will not be required to restrict an individual's personal data indefinitely but will need to have the restriction in place for a certain period of time.

See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/

The data that NetSupport DNA collects automatically is defined by the setting for the profile that is active when the user is logged onto a computer. If you need to disable any collection of data for an individual, you can create a profile and disable all data collection; this profile can then be assigned to an individual to stop NetSupport DNA collecting any information.

The right to data portability

The right to data portability only applies:

- to personal data an individual has provided to a controller;

- where the processing is based on the individual's consent or for the performance of a contract; and
- When processing is carried out by automated means.

See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/

This would not apply to any data processed by NetSupport DNA.

The right to object

The Guidance from the ICO states that:

"Individuals must have an objection on 'grounds relating to his or her particular situation'. And that you must stop processing the personal data unless you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual".

See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/

In the case of NetSupport DNA's eSafety and safeguarding features, this would be classed as compelling legitimate grounds for processing.

Rights in relation to automated decision making and profiling

The GDPR has provisions on:

- automated individual decision-making (making a decision solely by automated means without any human involvement); and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

NetSupport DNA does not perform any decision making based solely on automatized processing.

Some common questions

Is NetSupport the data processor or the data controller?

For a customer using NetSupport DNA, NetSupport does not have access to any school's data. Once the product is installed, all of the data is stored locally on the school's servers. Therefore, within the context of NetSupport DNA, NetSupport is neither the data controller nor the data processor.

However, if you enable DNA Cloud support, some personal data is replicated to the NetSupport DNA Cloud and, in this case, NetSupport Ltd would be a data processor for the personal data stored in the DNA Cloud. The Data Controller would be the school or organisation installing the software.

When enabling Cloud support in the DNA product, you have to agree to the NetSupport DNA Cloud Data processing agreement.

Is the school the data processor or the data controller within the context of NetSupport systems?

For users of NetSupport DNA, schools remain the data controller of their own data on the system.

Does NetSupport DNA process Personal Data?

Personal information associated with individual students and staff is processed by NetSupport DNA, therefore the rules of the GDPR apply to its use. This personal data is stored locally on the school's servers and therefore the school will remain the data controller and the data processor of this personal information.

When Cloud support is enabled, some personal data is replicated to the DNA Cloud and therefore NetSupport would be a data processor for this personal data

Does NetSupport DNA process Sensitive Data?

When an eSafety alert is triggered in NetSupport DNA, the system can be configured to record screen data and record images from a webcam. Due to the possible nature of this data, it could contain sensitive data, and as such, we recommend that this data be assumed as sensitive data.

Do I need to get consent from all staff and pupils before I can monitor them in school with NetSupport DNA?

No – you do, however, need to give a clear notification that the there is a monitoring system in place. This notification should explain that NetSupport DNA will record what they type and do, so staff and pupils understand what is monitored for safeguarding purposes. Schools should very clearly state why it is necessary to monitor students' access (and, where applicable, that of staff) and how that data will be processed, stored and deleted.

What if a child/parent doesn't consent to them being monitored in school?

As above, consent is not required. It is important to explain the need to monitor children in school and the reasons why. The ICO gives guidance on the lawful basis for processing information. See: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

The reasons will be a combination of public task (for maintained schools), legitimate interests (for independent schools) and the school's legal or contractual obligations, including child safety.

If you have any further questions regarding this document or any other queries regarding NetSupport DNA, please contact us:

General enquiries
+44(0)1778 382270
press@netsupportsoftware.com

Sales enquiries
+44(0)1778 382270
sales@netsupportsoftware.com

Technical support
+44(0)1778 382272
support@netsupportsoftware.com