GENERAL PRIVACY NOTICE

Content

Updated: July 1, 2020

Introduction

Bisnode AB is part of Bisnode Business Information Group. This Privacy notice provides high-level information about how we process personal data about you. You can also find complementary information on our webpage, www.bisnodegroup.com. The controller of the data described in this document is our local Bisnode company. For a full list please view our webpage.

How will we use the information about you?

Bisnode processes personal data for several purposes. Below you find a brief information about the purposes we have for our processing throughout the Bisnode Group. Please note that all purposes may not be used in all countries. For more detailed information please visit the country specific website: www.bisnode.xx

Purpose	Definition
Credit	Credit means that data is used for information about solvency reliability and creditworthiness. This should apply e.g. for providing credit scores and business information reports.
Directory	Like a catalogue with telephone number, subscriber information. Directory means that data is used for reference purposes.
Marketing	Marketing means that data is used for promotion activities to existing customers, sales prospects and other target groups. This should apply e.g. for selling address data to Bisnodes customers who in turns address marketing towards their customers.
Verification and control (data quality and data management)	This service contains updates, supplements and verification of personal information, also called data management and data quality. In this case Bisnodes customer normally wants to have their existing customer base updated with correct information.
Analytics	Analytics means that we use information about both individuals and companies to show how something has looked in the past or the likelihood that a company or a person will act in a certain way.
Compliance	Compliance means that data about you is used by our customers to fulfill certain legal requirements, such as knowing who you do business with and who is the real owner of a company.
Performance of contract	If you are a customer, an employee or a contractor of Bisnode we need to store certain information in fulfil the engagement.

What information do we store about you?

We process information about you as a consumer, as a sole proprietor and/or in your capacity as a decision maker at a company.

Basic contact data such as name, address, phone number, email

For **credit purposes** we store information such as income, taxes, real estate taxes, depts, payment remarks, bankruptcies and trade (payment patterns) information

For **marketing** we use basic contact data but, in some cases, we also do profiling. Profiling means that we add statistical variables about your likeliness, for example, to live in a household with children, lifestyle etc. These variables are not connected to you directly but rather a likelihood for a group of people that for example live in the same neighbourhood.

We have marketing information about both private individuals and people in their professional capacity, such as decision makers.

For **sole proprietors** we also store information about your business and its financial results.

Indirect information such as ownership of cars and real estate and information about your property/car.

If you use our **websites,** we also store cookie information to measure the traffic and behaviour on the site. Observe that only technical necessary cookies are stored by default, all others need your explicit consent.

Cookies, for further information about cookies visit www.aboutcookies.org or www.allaboutcookies.org. You can set your browser not to accept cookies and the above websites tell you how to remove cookies from your browser. However, in a few cases some of our website features may not function as a result. Bisnode uses Cookie Consent on all our home pages where only strict necessary cookies are set by default.

A more complete list of the data we have can be found on our webpage www.bisnode.com or go to the local www.bisnode.xx where xx should be replace with the two letters in your local country code. If you want details about exactly what data we store about you, please contact our customer service.

Where does the data come from?

Bisnode operate in many countries in Europe. Most of Bisnode's data come from

- Official sources such as tax registration offices, statistical agencies, governmental company registers.
- Telephone operators where applicable
- Other data brokers
- Partnerships with some of our customers around invoice information used to find payment patterns used for credit purposes
- Business related information used in our D&B offerings from countries where Bisnode does not operate come from our partner Dun & Bradstreet (www.dnb.com) and their worldwide partner network.

For details about which data we collect in each country please visit the www.bisnode.xx website (where xx should be replaced with country code).

Our legal ground for keeping the data

Legitimate interest for credit purposes

Please note that in some countries credit purposes are considered a public interest and there the reasoning below does not apply.

Credit information has a vital function in society. It allows companies to verify the ability to pay for merchandise ordered, for a bank to verify that a customer can pay for a house mortgage among many other things. In particular for contracts via internet, online shopping, etc. calculating and providing credit information (Bisnode's job) as well as receiving and using credit information (customers' purpose) can be seen nowadays nearly as a given and mandatory while executing such online contracts.

Bisnode keeps full registers of credit data to provide services for our customers to verify the credit status of an individual or business to help them manage their financial risks, such as minimizing the risk that credits are given to insolvent individuals.

In providing such service we also enable the following general interests in society:

- keeping down the debt on consumers - prevent over-indebtedness
- credit information is a vital enabler of the overall EU economy
- it is important for the economy that creditors can protect themselves against credit losses and for the credit applicants to obtain the requested credit
- it is important that the credit market and e-commerce is not restricted just because of the difficulties in assessing credit risks

Higher risk data

Bisnode considers and treats credit data as 'high risk' data in terms of compiling a large amount of data on each data subject - current debts and history of debts. The credit information database entails many data subjects. Bisnode does scoring for credit purpose but is never the one making the decision based on the score, manual or automatically, this is always done by the creditor buying the information.

Credit data is only used for credit related processing and never used by other Bisnode products.

Impact on the individual

Most individuals will not be granted a loan or credit if their solvency cannot be verified beforehand. For this reason, it is in the individuals' interest that credit information companies are available. However, an individual credit score can have negative impact on an individual if it is not based on correct information. In many of our markets data with higher risk than average (NOTE: not the GDPR definition of special categories of data) is stored to make the credit scoring calculations and to be able to show the general financial status of the individual. If this data for any reason is leaked it can be argued that it is a big intrusion into the privacy, even though the information in many countries comes from public sources.

It is also not to be expected that the individual understands the logic of the scoring or for example fraud solution based on a pattern, not facts. If these models are based on incorrect data, as previously stated it can lead to a denial of a loan, not being able to buy something on credit.

In the interest of the individual it is important to maintain a limited number of databases with credit data rather than each company giving credit having their own credit databases and to gather the data from authorities and other data sources themselves when credit information is required.

Provisional balance

It stands to reason that there are risks of intrusion into an individual's privacy. However, credit verification plays an important role with the paramount purpose of sound underwriting in every society. At its core and in

accordance with the consumer credit directive all credit institutions or companies providing credit of any kind shall make sure that credit is only granted to people who can pay back.

The data is protected and only used for the purpose stated. It is also in the interest of most individuals to be able to get a loan or a credit at some point in life.

Bisnode considers that the provisional balance is met when processing credit information as stated above.

Legitimate interest for direct marketing and data management

Recital 47 of GDPR states "The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest." Direct marketing is essential to most companies to spread the message about their products.

Bisnode's services within direct marketing and data management are to secure that our customers have data that is up to date and enough information to target the right customers, with the right message.

The Bisnode customer needs to find and correctly target individuals with product offers. There is also a need to know more about the individuals than just the contact details to personalize offers, target them at the right time (when they are most likely interested in the offer) and through the right channels. For that reason, more information than the customer has is normally needed.

Impact on the data subject – how may processing affect people's privacy

Keeping records of data subjects for the mean of direct marketing does not per se mean any affect to a person's privacy if the data is safe guarded.

Data impact

The data used for direct marketing is normally of basic nature and is not involving any high impact risk. However, when adding more information than traditional contact details, such as lifestyle variables built on statistics a clearer image of the person is built up. The more information collected or created the clearer the picture, hence higher risk. Bisnode does not store sensitive data as specified by GDPR about the individual.

Reasonable expectation of the individual

An individual will in most countries expect to receive direct marketing. They do expect that companies they have made previous purchases from to contact them again with new offers unless they have opted out. To some extent individuals are also expecting direct marketing from companies they do not have a relation with.

Marketing information to a B2B role (company representative)

Bisnode deems that it is not an intrusion into the individuals' privacy to send marketing addressed to their working role, (relevant marketing).

Impact on the individual

When processing basic contact data for direct marketing, Bisnode's view is that there is little risk that the processing may lead to high risk for intrusion to the privacy of the individual. However, there is always a risk that certain individuals do not want their information spread more than necessary and strongly object to this type of processing.

If the basic contact data is leaked or in other ways comes into the incorrect hands, there is low risk of harm as the data normally being publicly available. Other data (such as children, gender, civil status, date of birth) used for marketing can increase the risk, however it is still unlikely to do harm to the individual.

Provisional balance

Direct marketing is mentioned in Recital 47 of GDPR as a legitimate interest. Bisnode's processing of personal data is in many cases a necessity for our customers to find the right individuals, sending the right message, through the right channels. Bisnode is also very careful, following industry standards and codes of conduct for the processing.

Bisnode is always acting in line with industry standards and code of conducts as well as the right of opt out at any time and the use of Robinson lists, therefore an impact is very unlikely.

The foreseen objections from and risks for an individual will be mitigated through Bisnode's measures to handle the individuals' rights. No severe impact on an individual's privacy is expected with this type of activities. The consequence of wrongful information would be that the individual does not receive an offer via direct marketing, or that the person receives a message about an offer that is not relevant to her/him. This cannot be seen as very intrusive.

The main risk with processing data for direct marketing is the number of data subjects being processed within Bisnode and any potential leak of the information. This processing is protected by Bisnode's technical and organizational measures, view Appendix 1 for more information. We also classify all our data according to the C.I.A method. CIA stands for Confidentiality, Integrity and Availability and is used as a way of determining what security measures needs to be in place when using a particular type of data.

Bisnode considers that there is a legitimate interest for processing personal data for direct marketing purposes.

Legal framework

Whenever Bisnode processes personal data provided to us from an external part such as a Customer, Bisnode acts as a Processor of that personal data, processing on behalf of and by written instruction from the Controller in conjunction with a Data Processing Agreement.

For personal data that Bisnode have sourced for business purposes as described above, each Bisnode company acts as a Controller.

Whenever a Bisnode company acting as a Controller for personal data, using a service provided by another Bisnode company acting as a Processor, there is an intra-group agreement that regulates the safeguarding of the personal data.

In some rare occasions, typically for internal use, Bisnode act as a Group of companies where the Parties are part of the same Group, owned by Bisnode AB in Sweden. The Parties have a close cooperation in product development as well as Group Functions. Since the Parties will jointly determine the purposes and means of the processing of personal data in Group Products and other Group activities (including but not limited to Group Functions), the Parties has agreed to enter into a joint controllership agreement as per GDPR article 26 meaning that Parties, jointly are considered responsible for the processing of personal data.

Who do we share your data with?

Our business is to help our customer have the best possible data about their customers and to help them make sound business decisions based on correct data. Our customers operate in industries such as:

- Manufacturing
- Electricity, gas, steam and air conditioning supply
- Construction
- Wholesale and retail trade
- Information and communication
- Financial and insurance activities
- Real estate activities
- Professional, scientific and technical activities
- Administrative and support service activities
- Public administration
- Education
- Human health and social work activities
- TelCo
- Media, publishers
- FMCG
- Advertising agencies
- Partners and Brokers
- Medical

Subprocessors

Bisnode uses sub processors for handling our data in some cases. A typical scenario is our server providers that maintain our server environment, another is an external consultant company that helps us develop our solutions.

Bisnode takes great care in who we use to handle our data and have sub processors agreements in place that regulates how they handle our information. We also do security and technical assessments of our vendors to make sure they live up to our standards. You can read more about this in Appendix 1

As our sub processors work on our behalf, we are fully responsible for everything they do with our data.

How we secure your data

Bisnode complies with relevant industry standards and code of conducts. Bisnode also always use both internal and national mail preference service list (Robinson) to secure that anyone listed in these registers are not receiving unwanted marketing material by removing them from any customer lists sent out. A Robinson list is a list of people who have stated that they do not want marketing information. In many markets there are official Robinson lists available.

Please view appendix 1 of this document for further information on how we secure your data.

Store and Transfer

We take great care securing that all processing of our data takes place within EU.

In the few cases where we use processors outside EU, we carefully evaluate the processor, making sure that all necessary safety measures are in place and we always secure that we have the appropriate contractual terms in our agreements. For more information about technical measures, view appendix 1 of this document.

Your information is stored within the system for in accordance with our retention policies. How long we keep the data depends on legal requirements and business needs defined for each set of data. When it is no longer required it is deleted from our systems.

Your right to your data

Bisnode offers you access to the personal data we process. This means that the you may contact us, and we will inform what personal data we have collected and processed and the purposes such data are used for as well as about other important facts.

Right to rectification

You have the right to have incorrect, incomplete, outdated, or unnecessary personal data we have stored about you corrected or completed by contacting us. In some cases when we use official data, we might ask you to contact the authority directly to get your data corrected to secure it is done in the proper official manner necessary for those registers.

Right to erasure

You may also ask us to delete your personal data from our systems. We will comply with such request unless we have a legitimate ground to not delete the data.

Right to object

You may object to certain use of personal data if such data are processed for other purposes than what is necessary for the performance of our services or for compliance with a legal obligation. You may also object any further processing of personal data after prior given consent. If you object to the further processing of personal data, this may lead to fewer possibilities to use our services.

You have the right to prohibit us from using your personal data for direct marketing purposes, market research and profiling.

Right to restriction of processing

You may request us to restrict processing of certain personal data, this may however lead to fewer possibilities to use our website and services.

Right to data portability

You have the right to receive the personal data you have given us in a structured, commonly used format. Please note that this only applies to data that was given to us directly from you.

How to use the rights

These rights may be used by sending a letter or e-mail to us on the addresses set out below, including the following information: name, address, phone number and a copy of a valid ID. We may request the provision of additional information necessary to confirm your identity. We may reject requests that are unreasonably repetitive, excessive or manifestly unfounded. In case you consider our processing activities of personal data to be inconsistent with the applicable data protection laws, a complaint may be lodged with the local supervisory authority for data protection.

You have the right to request a copy of the information that we hold about you. If you would like a copy of some or all of your personal information, please email or write to us at the following address.

Email:	info@bisnode.com
Postal address	Bisnode AB 169 93 Solna

Right to lodge a complaint with the Data Protection Agency
You have a right to lodge a complaint with the Data Protection Agency if you are not satisfied with the way we treat your data.

Here you find the contact details to the Swedish DPA:

https://www.datainspektionen.se/other-lang/in-english/about-us/contact-us/

This is an extensive list to all EU DPAs:

https://edpb.europa.eu/about-edpb/board/members_en

Changes to our privacy information

We keep our privacy information under regular review, and we will place any updates on this web page. This privacy policy was last updated on 1 July 2020.

How to contact us

Please contact us if you have any questions about our privacy information or information, we hold about you

Call:	+46 8 558 059 00
Email:	info@bisnode.com
Postal address	Bisnode AB 169 93 Solna

If you need to get in contact with our Data Protection Officer use dpo@bisnode.com.

Appendix 1 – Technical and organisational data protection measures for Bisnode Group Products

In this appendix you will find more details about how we safeguard our data. Each Bisnode market has additional Technical and organizational measures for local processing.

Scope of application

Under the Data Protection Regulation (GDPR) any entity which collects, processes or uses personal data is obliged to take such technical and organisational measures as are necessary to ensure the implementation of data protection rules.

Entry Control

Entry control serves to bar unauthorised parties from gaining access to technical equipment by which personal data is processed or used.

Entry control at our operating premises
Entry to our buildings is regulated by admission controls. For our staff, these primarily consist of electronic keys which permit entry to operating premises according to the rights of access stipulated for each key. Rights of access are aligned with the powers granted to staff both timewise (according to permitted usage on certain weekdays and certain times of day) and location-wise (according to specific parts of the operating premises). For outsiders, entry control is ensured by a central reception lobby or doorman service which records visitors' data and issues visitors with visitors' passes valid for the duration of their respective visits.

Control of entry to our computer centre
Our IT systems are operated on behalf of us by different data centre. The data centres are designed as closed security spaces. There is both structural and technical admission control. The data centres are secured electronically and visitors are only permitted access when accompanied and are not left unsupervised. The entry cards required are only issued after prior notification and on strict terms and conditions. Usage is logged. The data centres are monitored by video and the site as well as critical internal areas of the building are also overseen around the clock by a security company.

Admission Control

Admission control encompasses measures by which the use of data processing systems by unauthorised parties is prevented (logical security).

Control of admission to our operating premises

Administrative work done by us or the data centre operator is only carried out by certain members of staff who have signed a special confidentiality agreement and been checked before being hired. The confidentiality agreement contains a commitment to data secrecy. Identification with usernames and secure passwords is obligatory. Our IT systems are also shielded from outside.

Control of admission at data centre operator

In order to secure the systems, run for our the data centre operator has installed additional high-end firewall functions within the network layer and admission products.

Access Control

Access control is the measures taken to ensure users only have access to data which they are allowed to access, and that personal data cannot be read, copied, changed or deleted without permission during the course of processing or use and after being saved.

Access control at our operating premises

We have defined and documented internal standards for the handling of permissions. These govern the rights that administrators have over systems run for clients. These set out, for example, the requirements concerning secure passwords.

Access control at data centre operator

Where the data centre operator is contracted by us to take over the setting up of users and authorisations at application layer it will in principle be bound by the same security standards as those applicable to our operating premises themselves. Deviations are only permitted if directed by us in writing. The definition of guidelines as to how application-specific authorisation concepts are to be designed by the data centre operator is determined by us.

Transmission Control

Transmission control encompasses measures to ensure that personal data cannot be read, copied, changed or deleted without permission during electronic transfer, whilst in transit or when saved on data media and that it is possible to verify and establish where personal data is to be transmitted using data communication equipment.

Transmission control at our operating premises

With regard to the general processing of data at our (staff data, supplier data, customer base data) transmission control (transfer control, transportation control, communication control) is ensured by way of appropriate technical measures. These include firewall, virus protection, VPN tunnel, data encryption and password protection for individual documents. Only suitable service providers are employed in the logistical

transportation of data. With regard to the commercial processing of data, especially the receipt and provision of its clients' data in the course of our information business, transmission control is ensured by logging all data processing stages. Where agreed with the client, data classified as particularly confidential is further encrypted for the purposes of transmission via public networks.

Transmission control at data centre operator
The data centre operator is bound by the same obligations regarding transmission control as we are. For operationally essential copies (backup), especially in the context of essential data security, only standardised and documented procedures are used. The production of all backups is logged.

Input Control

Input control encompasses measures to ensure that it is possible to subsequently verify and establish whether and by whom personal data in data processing systems has been entered, changed or deleted. Inputting may only be undertaken by staff who have access to the data. Logs of "certain process actions" on systems are also automatically created. The logging of "certain process actions" relates to processes which serve to ensure business continuity, which serve accounting purposes and the fulfilment of statutory retention requirements.

Availability Control

Availability control secures that personal data is safeguarded from accidental loss or destruction.

The basis of availability control is the outsourcing of the operation of IT equipment to the data centre operator's high-security data centre. They have redundant supply systems with an uninterruptible power supply and emergency generating unit (using redundant diesel generators, for example). Data availability, especially protection from data loss due to technical malfunction or accidental deletion, is also ensured through regular data safeguards and backups of all relevant databases and systems, so that in the event of a breakdown they can be restored on at least a monthly basis.

Separation Rule

The separation rule secures that data gathered for different purposes can be processed separately.

Separation rule at our operating premises
With regard to the general processing of data (staff data, supplier data, customer base data) the separation rule is implemented, for example, by a physical separation and storage on separate systems or data media, the separation of productive, testing and development environments for our applications and IT systems, appropriate authorisation concepts, as well as database rights. Furthermore, on the software side, a logistical client separation system is implemented.

Separation rule at data centre operator
The data centre operator separates all data both physically and logically at client level at least. When data is outsourced to the data centre operator there are generally further separate interfaces available based on a system or database.