Unified Communications and the EU GDPR

UC software helps companies protect their personal information

Transparency and accountability, deletion and anonymization, data minimization, integrity and confidentiality – these are the keywords that presently occupy almost all companies. By 25th May 2018 at the latest, companies must have implemented the EU GDPR guidelines, otherwise they face severe penalties. Software products used such as unified communications modules should support companies in complying with the GDPR.

Personal data in a UC software

The fundamental objective of the EU GDPR is the protection of personal data. Personal data is any data relating directly or indirectly to an individual or allowing conclusions to be drawn about them. Unified communications (UC) and CTI software bring together a wide variety of communication channels. The goal is to optimize, simplify and make more effective the internal and external corporate communication as well as work processes. Messaging features such as e-mail, fax, answering machine and SMS as well as computer telephony (CTI) and collaboration with caller identification, instant messaging, presence management, screen sharing and audio/video communication are provided under one user interface. Here, personal data is processed and stored in a variety of ways. For example, a fax message is provided with sender information, CTI requires at least one telephone number to provide the telephony features, and callers can only be identified if their contact is determined by the incoming telephone number from an in-house or external data source. Personal data is stored, for example, in the journal or in the log files.

Principles and obligations of the EU GDPR

The essential principles and obligations of the GDPR for the protection of personal data that are relevant for UC software are: appropriation, data minimization, transparency and accountability, accuracy of data, deletion and anonymization, storage limitation as well as integrity and confidentiality. Personal data may be used, processed or stored for a specific purpose. The data is limited to the purpose necessary. Upon request, a company must provide the person concerned with information on how the data is collected and in what form it is stored or processed further. If data is stored incorrectly, the problem must be rectified. Upon request, a person’s data must be deleted or anonymized, so that no further conclusions can be made about that person. As little personal data as possible may be stored by the company and only for as long as necessary. In addition, a company must take appropriate technical and organizational measures to ensure that personal data does not illegally fall into the hands of third parties. If this is the case, the regulatory authority and the persons concerned, with few exceptions, must be informed as swiftly as possible.

Appropriation and data minimization

Appropriation is automatically fulfilled by UC software. The personal data is processed or stored with respect to certain functions: In the UC client, the data is kept in the journal, for example, so that the user can see who has called and when, and which calls have been missed. In Favorites, the user saves selected contacts so that they can be called without having to search, connect via instant messaging or contact via audio/video chat. The UC server, in turn, accesses the corporate or external data sources only when the user has started a search or is receiving a call. The user receives the result either in the UC client or in the call window on the screen. The information from fax, voice or short messages is used for sender identification. The data stored in the log files is used by the administrator for error detection and correction. In addition, UC software such as estos ProCall Enterprise offers a number of possibilities to limit the processing of personal data in the sense of data minimization as far as possible: Depending on the information and purpose, only certain persons may access specific data. Only the administrator is allowed to access log files. Users assign privileges to their colleagues and other contacts and thus determine how far their data is minimized. You can assign these preconfigured groups, each of which has access to different detailed information. You can also assign individual authorizations. In the UC monitor, for example, the contacts see each other's data, such as telephone or mobile number, e-mail address, appointments and presence status. Here, individuals can allow members of their department to see who they are talking to, while others just see that they are engaged in a call. If a private telephone call is identified, it is generally not displayed.

Accountability, accuracy, erasure and storage limitation

Finding out what personal data is stored, how it has been collected and in what form, i.e. transparency and accountability, is another challenge. UC software supplies the data source in which search results information is stored, either in the UC client or the call window. However, it is cumbersome to look for them individually in this way. UC software such as estos' ProCall Enterprise provides a practical tool: All data processed and stored in the software, including data sources, is clearly displayed. On this basis, a company can conduct further research and provide qualified information about the collection, processing and storage of data. If the person determines that their data is incorrect, the company must rectify this. The more central the data management, the easier it is to ensure the accuracy of the data. If the software is administered centrally, it is sufficient only to change it in this one location. The changes affect the entire software. Data that is not stored in the UC software must be corrected accordingly in any external data sources, such as a telephone directory CD or the company's database. This is the only way to ensure that the wrong information does not appear repeatedly somewhere else. The same applies to the principle of deletion and anonymization: If a person requests the deletion of their data, they may no longer appear in connection or be associated with it. The central management of UC software ensures that the changes, such as deletion or anonymization, takes effect in the entire software. Personal data that the UC software obtains from external sources must be rectified here. If UC software generates a report on processed and stored data, including source information, the company can see the original location and can act accordingly. It is also helpful if stored data is automatically deleted when it is no longer needed. For example, personal data for troubleshooting is stored in the log files or in the journal. If the administrator has solved the problem, there is no reason to keep this data. In order to comply with the principle of storage limitation, UC software sets a reasonable period of time after the data is automatically deleted or anonymized. The administrator can change and adjust this period, either at installation or at any time.

Integrity and confidentiality

Security concepts in companies with firewalls, encryption, authentication and authorization protect against data theft and data breaches. In order to respect the principle of integrity and confidentiality with regard to the UC software, this must be integrated into the respective concept. A firewall protects the internal company network from external attacks and uses certain rules to check which data is allowed to pass through. If the components of UC software such as those of the ixi-UMS Unified Messaging Server from estos can be separated appropriately, the UM components that access the external network are on one side of the firewall and those that are needed internally for integration into the company’s network are installed on the other side. TLS encryption provides security for audio/video communication and chat with customers or suppliers, protecting peer-to-peer connections and instant messages. In addition, it is advisable to use a compliance procedure in the sense of authentication, for example, the challenge response allows the UC user to accept or reject contact requests. Different authorization levels make it possible, among other things, to limit the access of external employees to contacts in the company network.

Conclusion

Unified communications software enhances communication and collaboration across the company and across company boundaries. As a building block in the ITC structure of the company, it is also a building block on the path to conforming to the EU GDPR. If the UC software complies with the principles and guidelines and provides practical tools for researching personal data, it facilitates the company's ability to implement the criteria of the European General Data Protection Regulation.

About estos
estos – enables easy communication
estos GmbH is an independent manufacturer of innovative building blocks for unified communications. Since 1997, estos has been developing professional standards software for small and medium-sized companies, thereby improving their business processes in communication-intensive areas. As a technology leader, estos has demonstrated its expertise in the area of Computer Telephony Integration (CTI), Unified Messaging Software (UMS), SIP, XMPP, LDAP and WebRTC-based applications that enable uncomplicated audio/video communication. estos has constantly invested in research and development helping to create innovation and ensuring their products are the forefront of genuine trend-setting technology. The core markets of the company are Germany, Austria, Switzerland, Benelux and Italy. estos GmbH is headquartered in Starnberg, close to Munich, and operates a Knowledge Center Messaging in Olching, a development office in Leonberg, an office in Berlin and branches in Udine, Italy and Doetinchem, in the Netherlands.