



Privacy by Design

Building business collaboration in
accordance with the GDPR regulation

Whitepaper

Privacy by Design
January 2021

Privacy by design: Creating trust

Today, employees, partners and customers are able to collaborate wherever they wish due to social networks and the ability to communicate in real time. But not all communication tools provide the necessary framework to address continuous availability, security rules, confidentiality, and compliance.

Organizations need to provide employees with an agile, robust and resilient solution. They need to end the proliferation of consumer services that deliver data from employees, partners and customers to web giants.

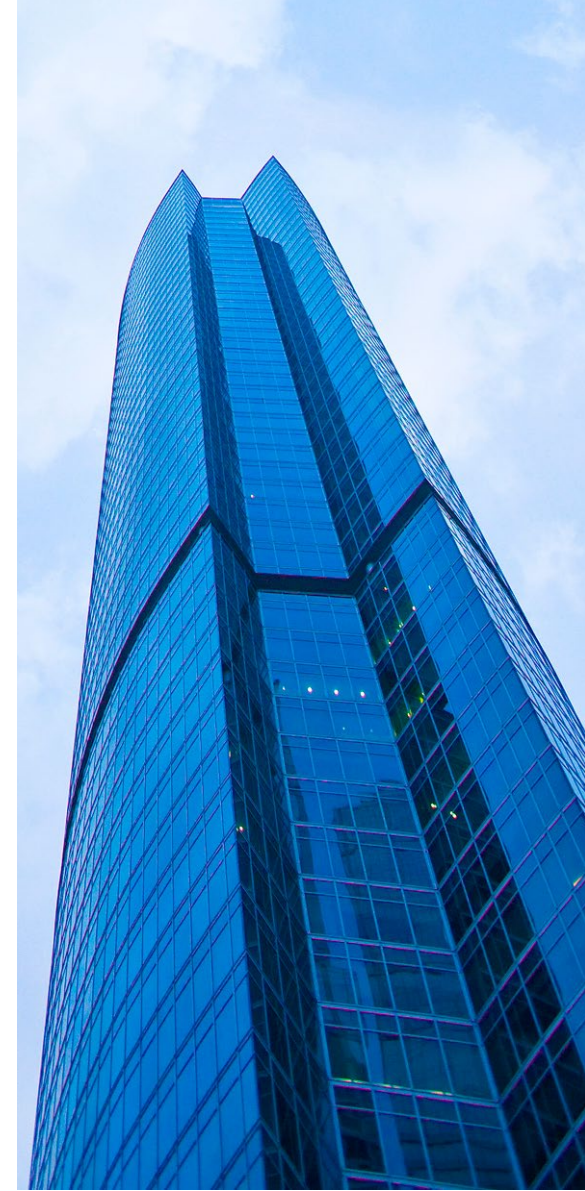
The question is, how do you transform real-time information flows into exchanges that are beneficial to your organization and no one else, while at the same time maintaining the confidentiality of personal data?

This white paper provides a methodology for building a platform to connect people, services and objects. It is a step-by-step

guide for delivering scalable exchanges that comply with the latest European General Data Protection Regulation (GDPR) and ePrivacy regulations.

The underlying principle is simple: The person concerned (the data subject) owns their personal data and no one else can freely dispose of it without such person's consent. The GDPR organizes ways to ensure that the person concerned enjoys their full rights and that the collection, or processing of data, by third parties is subject to such person's prior consent, or is pre-empted by higher ranking legal provisions.

Please feel free to share this document. We hope it helps your team create a culture that includes the thoughtful use of unified communications while keeping their exchanges safe from prying eyes and web cookies. In addition, you can avoid risking denial of service attacks, fraud and sensitive data leaks.



Four steps for a successful project

1. Build a trusted collaboration infrastructure.

This phase provides a solution prototype that an initial group of users can use to test the chosen solution.

2. Study the impact on the company and its ecosystem.

After review, the collaboration solution can be expanded to partners and/or customers.

3. Adopt the latest digital trust standards.

The company maps its data, uses, and processing managers then traces the exchanges, thus limiting the risk of sensitive information being leaked.

4. Bring together the key factors of a successful implementation.

At the end of this step, the platform provides a personalized collaborative work solution, improving team responsiveness and productivity.

Build a trusted collaboration infrastructure

The four simple steps that comprise the Privacy by Design approach are key in the success of your project to build and maintain digital interactions that are both effective and in compliance with the latest personal data regulations.

The European GDPR regulation is effective on May 28, 2018. It concerns any organization collecting or hosting personal data that can be used to identify a resident of the EU directly or through a third party. A well-controlled information system with traceable data processing and data flows will support GDPR compliance. The question is how do you regain control of data, mobile devices and shared online services that have been accumulating over the years? You regain control by building a base of compliant exchanges and removing the risks introduced by BYOD (bring your own device), shadow IT, and SaaS solutions (Software as a Service) retained outside the information systems department (ISD). "Complying with the GDPR regulation requires identifying and managing different types of data, including personal data. Compliance also requires the anticipation of crises and the ability to respond based on the gravity," suggested Louis-Philippe Ollier, Data Protection Officer at Alcatel-Lucent Enterprise.



A secured infrastructure foundation

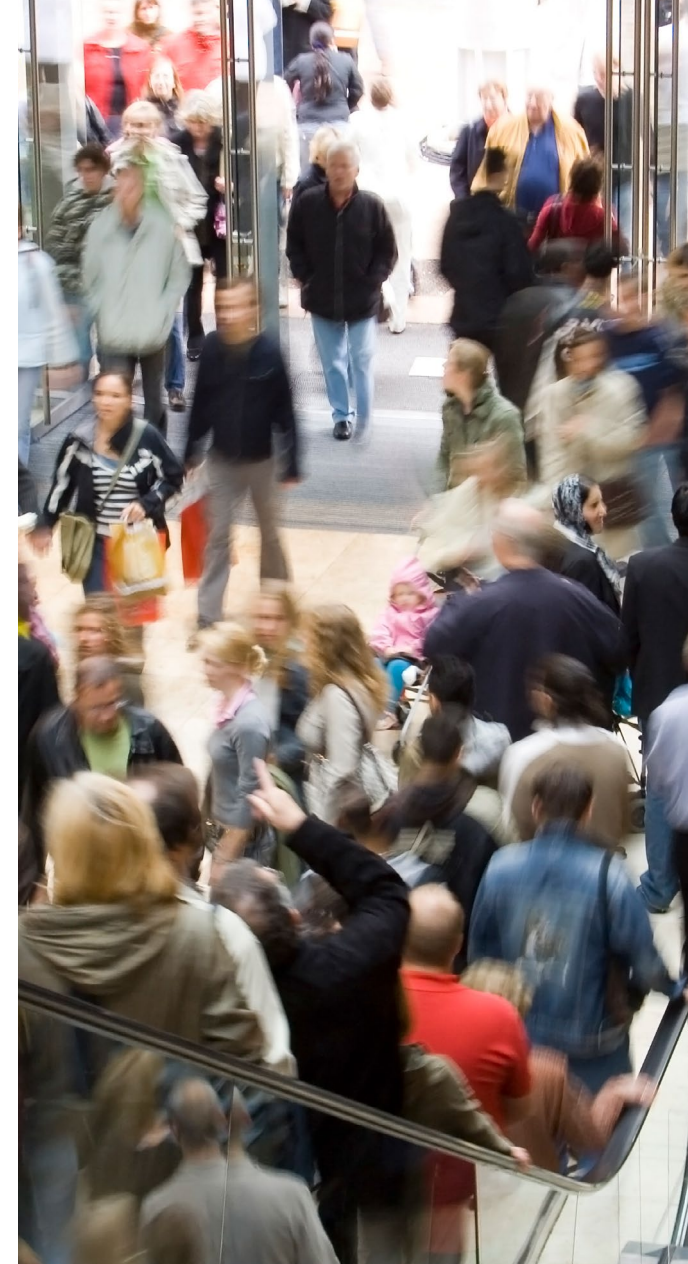
Collaboration requires a reliable infrastructure foundation. The network must support large applications such as videoconferencing, desktop sharing as well as professional documents. This infrastructure can be delivered on a turnkey basis and managed by an internal team or managed by a service provider on behalf of the company.

In a digital collaboration project, the initial goal often varies by organization. Requirements can include the need to schedule remote meetings, share and synchronize files, and accelerate the exchange of expertise and ideas through a corporate social network. Real-time communications can improve the productivity of geographically dispersed teams, reduce travel costs and streamline internal procedures. Networks are expanding rapidly making it increasingly difficult to define the perimeter. A network could encompass cloud hosts and service providers, branch connections, telecommuting employees and mobile links, making access and data protection an inevitable priority.

A local technical partner

Regardless of the device used, the collaboration solution must be able to receive, store, process and protect the personal data of each employee, at a state-of-the-art level. "Many companies now see a real and valuable opportunity to subscribe to a local, European operator who is committed to adhering to the principles and commitments of the GDPR. This coincides with our strategy to create connected equipment and operate remote platforms for our customers. In doing so, we are taking more responsibility for data by becoming a cloud service provider, and must therefore guarantee the best possible protection," acknowledged Vincent Lomba, Chief Technical Security Officer at Alcatel-Lucent Enterprise. Alcatel-Lucent Enterprise is a proud partner of local organizations and companies of all sizes around the world.

In addition to supporting users, it is important to ensure successful integration of the solution into the enterprise and the applications already in use. The adoption of open standards and APIs, can provide a smooth transition, while a collaboration platform can help automate repetitive tasks that have little added value for employees. In addition, new and innovative services can be deployed to support the organization's digital transformation.





A chatbot can save time

A chatbot is a conversational agent designed to assist after-sales service or technical support, direct the user to the right online resources and answer frequently asked questions without human intervention. While communication platforms employ these types of automation, the ability to easily customize them is necessary. Advanced machine learning features enhance the understanding of the questions asked in a natural language. They can also participate in the automatic generation of questions and answers. The combination of artificial intelligence engines, together with the Alcatel-Lucent Enterprise Unified Communications and collaboration offering, enables these powerful services to be delivered in a unique manner.

Professional skills remain the exclusive domain of human collaborators to whom the chatbot provides time-saving assistance. Real-time interactions between employees, partners and customers provide more satisfaction to everyone. The platform to be built should not replace human interactions, but rather support them while maintaining the integrity of the exchanges. The creation of chatbots provides benefits but also introduces new risks. The methodology outlined in this document can assist in anticipating risks. Alcatel-Lucent Enterprise implements the methodology once the requirements of the chatbots are defined.

“Preparing for the GDPR regulation means recognizing and accepting the importance of processing personal data. One difficulty is identifying the data in collaboration flows conducted in real time. The Alcatel-Lucent Enterprise Rainbow solution data dictionary (the data model) makes it possible to know precisely which fields and procedures make use of personal data. This is a key element of our Privacy by Design approach.”

– Louis-Philippe Ollier

Study the impact on the company and its ecosystem

In the face of risks, such as a breach of confidentiality or of integrity associated with a data transfer, crisis management protocol and impact analysis are two measures that can be implemented. Specific responses can be monitored, depending on the importance of the information.

According to the GDPR regulations, every individual has different rights regarding their personal data. Employees can ask their organization about individual rights (right of access). The individual may also request the deletion or modification of specific data, (for example, identifiers), personal details, or preferences regarding online services. This fundamental right includes objecting to, or limiting, all or parts of the processing purposes, to protect the privacy of the citizens of the European Union. In practice, the destruction of records is not the only possible option. For example, some information can be made anonymous, or names can be replaced by pseudonyms before undergoing analysis.

However, the monitoring of information and applications is becoming a requirement. The European regulation encourages the keeping of a register that tracks the processing and cartography of personal data. It also provides information pertaining to how a user can request a change, or destruction of their personal data.

Data control and reporting

Beyond the inventory, several data protection technologies are periodically used. For example, information encryption is one of the tools commonly used in internet transfers. Other ways of filtering data or protecting access may be used in addition, each focusing on one layer of the information system (infrastructure, virtualization and applications). At the same time, best practices must be exercised by development teams.

“We respond to customers who question us about compliance, with information security standards such as ISO 27001 or the GDPR. Our design methods and our organization integrate the founding principles of these normative and regulatory frameworks at a very early stage. This extends from our technical development and operations teams to the sales teams in charge of defining the offers and supporting our customers.

Confidentiality required by governments and other sensitive sectors is addressed in the technical design of our products and software, as well as in our organizational procedures. These privacy requirements are increasingly becoming a part of the basic foundations requested by our partners and customers as we approach May 25, 2018,” says Vincent Lomba.

Organizations that purchase IT services need to assess the security and privacy commitments to which cloud providers are bound under contract. These guarantees are necessary for companies with partially outsourced applications because they remain liable for the entire information processing chain. The companies must be able to specify the means and procedures for protecting personal data, using updated reporting. Companies that offer its employees and subcontractors access to pre-selected services that provide safety and compliance can curb shadow IT.

The obligation to alert within three days

In the event of a cyber attack that has caused a leak of private information, the company must notify the personal data protection authorities (such as the CNIL in France) within three days once the incident has been discovered. If the personal information is usable, the employees or customers concerned must also be informed, irrespective of the number of breaches. Significant penalties can be levied in the event of non-compliance with the GDPR regulation. This is to encourage all organizations to set up controls, as well as accurate and regular reporting associated with protecting private data. The sanctions are intended to incentivize companies to comply. They can trigger a fine of up to 20 million Euros or up to four percent of the total annual revenue of the company, whichever amount is higher. The financial risk becomes considerable. Not only will the company's reputation be tarnished in the event of a successful cyber-attack, but the legal risk can trigger a financial cost that could jeopardize the company's survival.



“Rainbow collaboration services are operated in France by local teams who are aware of the GDPR regulations and who demand compliance. The level of confidence provided by the European regulation, one of the most concerned with individual rights, provides superior confidentiality compared to a cloud service hosted outside of the territory. The European Union is becoming a global standard in this area. It is common knowledge that operators in other regions do not provide the same level of confidentiality when processing personal data and when responding to access requests authorized by local laws,” says Vincent Lomba.

By opening the information system to partners or large customers, the company can transform these stakeholders, into brand ambassadors. The company can deploy personalized online services, offer direct and spontaneous interactions, which can contribute to the improvement of products and services on a global scale.

“ Rainbow has been developed in parallel with the GDPR regulation - it’s fundamental to the design. We take great care to maintain the confidentiality and anonymity of users in to ensure the field is not exposed to unauthorized analyses and especially that the confidentiality rights of our users are not compromised. From an organizational point of view, very early on, we established in-house workshops to incorporate domain awareness into the life cycle of our projects, with impact analysis and key checkpoints in which DPO representatives participate. ”

- Vincent Lomba

Preparing for cyber attacks

Threats go beyond the scope of the IT department. Research firm PricewaterhouseCoopers suggest, Senior leaders driving the business must take ownership of building cyber resilience. Setting a top down strategy to manage cyber and privacy risks across the enterprise is essential.”

In a recent study of 9500 executives in 122 countries, PwC revealed that companies are often not prepared to properly respond to cyber risks. 54% do not have an incident response procedure, while 48% do not have an employee security awareness training program. In the event of a targeted attack on an automated production system, 40% fear a lasting interruption, and 39% cite the compromise of sensitive data, 32% cite harm to product quality, and 22% cite harm to human life.¹

¹ <https://www.pwc.com/id/en/media-centre/press-release/2017/english/organisations-are-failing-to-prepare-effectively-for-cyberattack.html>

Adopting the latest digital trust standards

Digital trust is based on control, traceability, and the audit of interactions. The classification of the data makes it possible to appropriately store and protect it, according to its value, at every moment.

An impact study showed that personal information is typically stored in multiple places: Internally, at the home of telecommuting workers, or at the host.

Beyond a selection of trusted partners, the inventory and data mapping help place files in the right place, at the right time and based on predefined rules.

Just as one wouldn't enter bank details or access codes just anywhere, different strategies for storage, backup, replication and transfer, with or without encryption, are created to match each class of data.

Trust and responsibilities

Everything that enters and leaves the computer or the corporate network generates digital risk such as, fraud, attacks, and information seepage. IP communications amplify this phenomenon. "Business conversations often contain confidential information.

We must organize ourselves to ensure compliance," Louis-Philippe Ollier confirms.

The field of responsibilities has evolved. In the past, a simple verbal agreement was enough for two people to secure a contract. Now, two, and often more, corporate entities are bound by online signed service contracts. They are sometimes certified by a trusted third party, notary or lawyer, but more often than not, it's just a simple click on a web form. The question of how these contracts are maintained is an interesting one. Strictly speaking, a timestamp token, a record of the file and an electronic signature should prove the authenticity of the issuer, the integrity, and the date and time the document was written. And, it should be stored at a trusted third party. Digital trust should even be expanded to include surveillance and artificial intelligence. The same applies to the legal, ethical and moral responsibilities of business managers who deal with private data.

Double conformity in the European model

The European GDPR and e-Privacy regulations are not exhaustive. The goal is to bring "more control, more choice and more consent from the user who needs to be better informed about what is actually being done with their digital data," says Nataliia Bielova, a researcher at INRIA. She explains that this knowledge is essential, and a prerequisite to being able to give, or withhold, user consent for computer processing. Examining web tracking and monitoring technologies, is enabling Bielova to develop user-friendly tools for online service developers.

"The sanctions provided in the event of non-compliance should encourage companies to recruit people who are aware of these rules. These people will need to ensure their company information systems comply with both regulations at the same time," she indicates.

Before the GDPR, each country of the European Union translated, at the national level, the directives adopted by the European Parliament, then by the European Commission. This created a very heterogeneous set of rules. In addition, national and European laws were supplemented by the professional branch regulations. This additional compliance imposed difficulties implementing specific features or configurations that were required for specialized industries such the financial or health sectors. In response, the GDPR offers unified regulations that apply to all member states as identified in the document.



Encryption and data flow protection

At the digital exchange level, security protocols and encryption enable the addition of confidentiality, authentication and integrity guarantees. Communications security is enhanced through access controls, for example, through user authentication using several factors, such as biometrics.

These technologies are becoming increasingly popular at the right time. Content and service providers are now left to decide on the implementation in the architecture. The GDPR regulation suggests, but does not impose technical solutions. Rather it highlights the liability of all stakeholders in the system with regard to the respect for privacy. Preventive measures guarantee the integrity and the protection of the information, with the addition of the processing transparency, the consent of the user and the regular follow-up of confidentiality requests.

“Ideally, I would like guarantees on each software package used, including the verification tools and certificates proclaiming respect for privacy. In addition, all rules to obtain this seal of trust should be transparent,” notes Nataliia Bielova.

“ The GDPR invites organizations to demonstrate e-security solutions that have been successfully implemented in the prevention of personal data leakage. With Rainbow, we know that our hosting provider’s equipment is physically secure and that logical access is protected. In addition, we provide proof that we are implementing the most advanced security measures to protect our customers’ data. This allows them to integrate these measures into their own security policies. ”

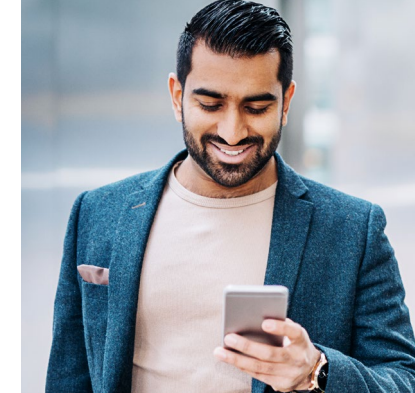
– Louis-Philippe Ollier

What will the ePrivacy regulation change?

The right to escape any electronic surveillance is vital from the perspective of democracy,” says Marju Lauristin, MEP, author and rapporteur of the ePrivacy Regulation, which replaces the previous directive (2002/58/EC). On October 19, 2017, the text was voted on by the European Parliament after several weeks of intense discussions. Its implementation will transform the current practices on the Internet. Specifically, the Privacy by Design approach will be necessary to create new services. The traceability of internet users will not be permitted without their prior consent. Encryption will be mandatory when transferring data and private conversations on the internet. Service providers or third parties operating without provisions for user consent, or confidentiality parameters for cookies may incur sanctions equivalent to those of the GDPR, representing up to four percent of the total revenue or 20 million Euros.

Bringing together the key factors for a successful implementation

Depending on the data processed by the company, special rules for storage, analysis and archiving may be defined. Below is a review of the best practices for the successful implementation of a trusted collaborative platform.



The collaboration and unified communications platform is an important foundational tool for the company. However, the return on investment only becomes evident with the enrollment of each working group. To make this happen, the stakeholders must be consulted, and their concerns taken into account and addressed. The project initiation involves consulting with all stakeholders. Some employees are already familiar with collaborating in real time. Others require support and reassurance. Consensus must be reached to define the objectives and desired benefits of the project.

An intuitive user experience

Too often, security measures hamper the regular use of innovative new services. When it comes to collaborative work, the user experience must remain intuitive. For example, with Rainbow, starting a new group (known as a bubble), an audio

video conference, or a screen-sharing is simple and immediately effective. And it doesn't require any technical support assistance.

"When employees sign their employment contract they accept the terms of use associated with their employer's communication and collaboration system. In this context, there is no requirement to post a notice requesting their consent at each session," observes Louis-Philippe Ollier. However, automatic processing aimed at profiling internet users should require user consent. Better still, anonymous data may be even more desirable.

On the administrative side of the solution, an increasing number of settings are becoming end-user accessible. The combination of terminals used and preferences provide many possible combinations. Self-learning and self-service can be encouraged, through

the use of tutorials and online help that provide system best practices.

In organizations spread across multiple sites, it is important to verify platform compatibility based on environments approved by the IT department, including for example, the allowance of mobile apps for Android smartphones and IOS tablets. In addition, the collaborative solution and the automatic exchange (PBX) dialogue through the API to facilitate the management of telephone services and exchanges in real time. This evolution is leading design teams to more upstream control.

"Previously, a product was developed and then tested for security validation before being released to the market. DevOps models required the implementation of security controls in the early design stages. This is important to ensure that developers are aware of the security requirements throughout all design

phases of the project. Our industries are required to develop a DevSecOps approach by integrating the teams responsible for security for a more holistic design approach," says Vincent Lomba.

A flexible business model

The collaboration platform must be adaptable, flexible, transparent and secure all at the same time. The supplier must have the requisite financial base, durability, reputation and a network of partners, close to where the business operates, and offer the same level of services.

The ability to choose a private cloud deployment, or alternatively a SaaS model (Software as a Service) allows the customer to adopt a platform according to their current IT and financial strategy. The SaaS model lets the buyer reduce the TCO and transform a traditional investment into a service subscription, with a fee-for-service billing. There is no additional hardware investment in anticipation of potential increases in demand. The elasticity of the cloud makes it possible to spend based only on what the collaborators really use. The administration of the solution is left to the cloud service provider. In private or hybrid cloud mode, the financial and IT managers are able to finely monitor the uses and resources actually consumed.

Due to compliance with the primary industry standards and with the proposed API, the collaborative platform remains customizable. The Privacy by Design approach facilitates the composition of new secure services, from their design phase, to their implementation at all sites. Other benefits include automated workflows, improved business processes, and rapid integration of web services and business applications.

“ Our customers expect us to support their ability to achieve compliance when they use our products and services, including vertical solutions for sectors such as health or finance, or for government markets that need to add their own security requirements. The GDPR principles call for further consideration of the use of encryption of personal data for its protection, and the use of anonymous or pseudonyms in the creation of data models and architectures. ”

– Vincent Lomba

The DPO supervises the protective actions

By appointing a data protection officer (DPO), the company indicates its desire to have a point of contact with the authorities such as the CNIL in France. This internal resource is focused on bringing the company into compliance and maintaining its compliance. The DPO must ensure that:

- The regulation is well known and understood by internal and external stakeholders
- Personal data is identified and the processes using such data are identified and managed in the appropriate register
- The company understands, based on the definition of the products or services, the necessary functionality at the service, the principles, and the rights of the person concerned (the data subject)
- All of the stakeholders have access to the DPO: The data controllers, the subcontractors and the external authorities (the CNIL in France).

While bearing in mind the economic, legal and technological challenges, the DPO regularly engages with the information system manager, and the security and IT production managers to implement the proper measures while guaranteeing confidentiality and integrity of information. The DPO ensures compliance with the European regulations and propagates the good practices adopted by the business branch of the company. In doing so, the DPO helps anticipate and manage possible incidents, for example, by approving new surveillance measures. On a day to day basis, the DPO and its counterparts work to continually improve the security and confidentiality levels of the information system.

Glossary

Accountability: This refers to the responsibility and accountability of the company to the public authority to implement the GDPR and ensure that the implementation is effective and enforceable. As a corollary, it refers to the obligation of the company to implement internal mechanisms and guidelines to demonstrate compliance with data protection rules, including crisis management and responses to personal data leaks.

API: Application Programming Interface. The standard entry point for software that provides internal services to other programs, either through web services or through a library of classes, methods, or documented functions.

BYOD: Bring your own device. The practice of bringing your personal communication

equipment (smartphone, tablet, laptop, connected objects) into the professional environment. The associated risks, concerning the security of the network and the leakage of sensitive data, lead the company to abandon it in favor of the COPE approach (read below).

Cloud computing: Cloud computing is a form of relocating the infrastructure, computer platforms and software. This technical and economic model offers the rental on-demand services, computing capabilities and storage space distributed on servers connected to the Internet.

CNIL: The Commission Nationale Informatique et Libertés is a complete and agile regulator, driving the digital inter-regulation in France and Europe (https://www.cnil.fr/sites/default/files/atoms/files/plan_strategique.pdf). Article 1 of the Act on Information Technology and Civil Liberties states: "Everyone has the right to decide and control the use of their personal data."

COPE: Corporate owned, personally enabled. This practice, which allows private access to a company-owned terminal, is preferable to BYOD because it facilitates control and monitoring of devices in compliance with the company security rules.

Cryptography: Cryptography is a discipline designed to ensure the confidentiality, authenticity and integrity of messages through the use of secrets or secret keys.

DPO: Data Privacy/Protection Officer. Responsible for the protection of data, the DPO is in charge of the implementation of, and compliance with the European regulations as it pertains to the processing of personal data. This job function, sometimes associated with the legal department, may be executed by the former CIL, Correspondant Informatique et Libertés (The IT and Freedoms Correspondent).

GDPR/RGPD: General Data Protection Regulation. This European regulation aims to protect the personal data of individual EU residents and define principles and enforceable rights. For example, it regulates inter-company data transfers. More information available at: <http://eur-lex.europa.eu/legal-content/EN-FR/TXT/?uri=CELEX:32016R0679&from=FR>

ePrivacy: Directive on Privacy and Electronic Communications, which seeks to better protect browsing data of Internet users with a high level of protection throughout Europe. More information available at: <https://ec.europa.eu/digital-single-market/news/eprivacy-directive>

Shadow IT: Information processing service chosen, sometimes to test a concept, without the consent of the information systems department. With no guarantee of availability or security, they introduce risks of inconsistency, loss of data and non-compliance.

Continuous and spontaneous interactions are essential to the responsiveness of any organization. When employees are reachable and their availability is displayed on their smartphone, computer or IP phone, this can facilitate the sharing of knowledge, and improve partner and customer satisfaction. The current regulatory environment (GDPR and ePrivacy) requires governance, including the mapping and processing of personal data. It is important for the company to define its own impact assessment scorecard, establish its own security rules and provide appropriate responses for the protection of personal and sensitive data. Digital trust cannot be decreed. It is established with local partners capable of supporting their customers wherever they are and who are concerned about complying with the European regulations.

Useful links

- Alcatel-Lucent Enterprise Rainbow website: <https://www.openrainbow.com/>
- Alcatel-Lucent Enterprise Rainbow data privacy: <https://www.openrainbow.com/dataprivacy/>
- ALE Corporate privacy policy: <https://www.al-enterprise.com/en/legal/privacy>
- Mobile App Alcatel-Lucent Enterprise Rainbow for IOS: <https://itunes.apple.com/us/app/ale-rainbow/id1053514112>
- Mobile App Alcatel-Lucent Enterprise Rainbow for Android: <https://play.google.com/store/apps/details?id=com.ale.rainbow>

Twitter: <https://twitter.com/aluenterprise>

LinkedIn: <https://www.linkedin.com/company/alcatellucententerprise>

About ALE

We are ALE. Our mission is to connect everything to create the personalized technology experiences that customers need. On your premises, in the cloud or in a mixed model, we provide effective network and communication solutions for your people, processes and customers.

With its tradition of innovation and dedication to customer success, ALE is a leading provider of network and communications solutions and services with more than 830,000 customers worldwide. Due to its global presence and local operations, more than 2200 employees and over 2900 partners in 50 countries operate under the Alcatel-Lucent Enterprise brand.

The Alcatel-Lucent name and logo are registered trademarks of Nokia used under license by ALE.

