General Data Protection Regulation (GDPR)

Compliance Guide

PoliteMail®
for Outlook Email Intelligence™

Recognizing Employee Data Privacy

With less than six months left for GDPR to come into effect, Michael DesRochers, Founder and Managing Director at PoliteMail Software explains how HR teams must prepare for the incoming EU General Data Protection Legislation.

Less than a year away, on May 25, 2018, companies with employees based within the European Union (EU) must be in full compliance with the EU General Data Protection Regulation (GDPR). The intent of the GDPR is to assure the privacy of EU residents and facilitate the appropriate use and secure transfer of personal data.

The GDPR enhances the prior EU Data Protection Directive by better defining what constitutes personal data, adding breach notification requirements and significant penalties for non-compliance. The GDPR requirements are also far broader than the previous legislation and includes consent requirements to collect personal data and data protection requirements for cloud service providers.

The penalties for noncompliance are severe, with fines for violations of up to 20 million Euros, or 4 percent of the company's worldwide revenue, whichever is greater. For those companies in the US collecting or processing data of EU citizens, the former Safe Harbor privacy principals have been replaced with the EU-US Privacy Shield framework.

Employee data is personal data

Most of the awareness around GDPR has been focused on the privacy of customer data, yet companies cannot overlook employee data. For any organization with citizens of the EU as employees, how such employee data is collected, processed and stored definitely falls under governance of GDPR. Human resources teams for multi-national companies are quickly realizing GDPR compliance for EU employee data is shaping up to be a major challenge – possibly more so than for customer data.

First, it's important to understand how personal data is defined under the regulations. Data means information that is being processed and/or recorded, whether automatically by digital interactions or manually via paper forms and files. Personal data is related to a living individual who can be identified:

a. from those data directly, such as name, ID, email address or phone number, or

b. from those data and other information in the possession of, or likely to come into the possession of, the data controller, and

c. includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

If you have employees or clients in the European Union you will have to ensure that the data held on them is GDPR compliant.

The GDPR also defines other categories including "Sensitive Personal Data," which include ethnic, racial, religious and political information, health information including genetic or biometric data, sexual orientation and even union membership. Data related to criminal offenses, common to employee background checks, may only be kept by responsible national authorities.

It's important to know that personal data includes being able to make a conclusion about the identity of a person even without specific personally identifiable information. An example given by the UK information Commissioner's Office is, "a combination of data about gender, age, grade or salary may well enable you to identify a particular employee even without a name or job title."

Under GDPR, personal data can be defined if an individuals identity can be deduced from a combination of data.

Recital 26 of the Directive states that whether the individual is identifiable will depend on "all the means likely reasonably to be used either by the controller or by any other person to identify the said person."

- Three other important terms to understand regarding GDPR are the data subject, the data controller, and the data processor.
- The data subject is the person from whom or about whom the data is collected.
- The data controller is the organization, operating under EU member state laws, that is determining the purpose and means of processing person data and who bears the primary responsibility for compliance.

The data processor is providing data services (such as collection, transmission and/or storage) under explicit direction of the data controller. For purposes of the regulation, the company is the data controller, and that company's system provider is the data processor. Both have responsibilities to respect and secure that data.

HR teams that use tools to collect resumes containing personal information of prospective empoyees must adhere to GDPR.

Given these definitions, it's clear that any data a company collects about an employee or prospective employee should be considered personal data. HR teams that use tools to collect and process resumes and make comments regarding those resumes must understand that any of this information is covered by GDPR. When companies are collecting personal data for benefits enrollment, for example, and storing that in HR systems, it is all considered personal data. The same goes for any communications systems, including corporate email. Essentially, assigning a business email address to an employee is creating personal data. If an employee's name, title and email have been stored in an Active Directory, that is processing personal data.

If all employee data is personal data, what do we do about it?

While much of the required compliance actions shall be legal in nature, such as changes to employment and privacy agreements, updates to policies including acceptable use, technical and security measures, and changes to breach notification procedures, anyone involved in handling employee data needs to understand the compliance requirements and implications.

Steps to Compliance

The whole point of the GDPR is that personal data belongs to the person, and not those collecting and processing it. This means respecting the privacy of the individual, and not sharing any data without their consent. And, if that data does happen to leak out, both the data controller and the data processor have responsibilities to notify the data subjects within certain timeframes.

Generally, data collected in the EU must stay in the EU, unless the country of transfer ensures an adequate level of data protection. These countries are currently limited to Argentina, Canada, Switzerland, Israel, Isle of Man, New Zealand and Uruguay, and to the US when such transfer is to an organization certified under the EU-US Privacy Shield program. For multi-nationals, data may be transferred within a corporate group by way of Binding Corporate Rules, as approved by the national Data Protection Authorities (DPA's).

Redefining Legitimate Interests and Consent

Most businesses rely on boilerplate privacy policies and employee agreements to obtain consent to collect and process information. However, under the GDPR, merely agreeing to be an employee will not be deemed voluntary or freely-given consent, because of the unequal bargaining positions between employers and employees.

Boilerplate privacy policies of the past will no longer be adequate under the new General Data Protection Regulation.

Employers will now have to be much more transparent about what data is being collected, why they are collecting it, and how they intend to use it including who shall have access to it.

This should not consist of privacy policies that are excessively lengthy or difficult to understand, as the GDPR requirement is for controllers to provide concise, transparent, intelligible language that is easily accessible to employees.

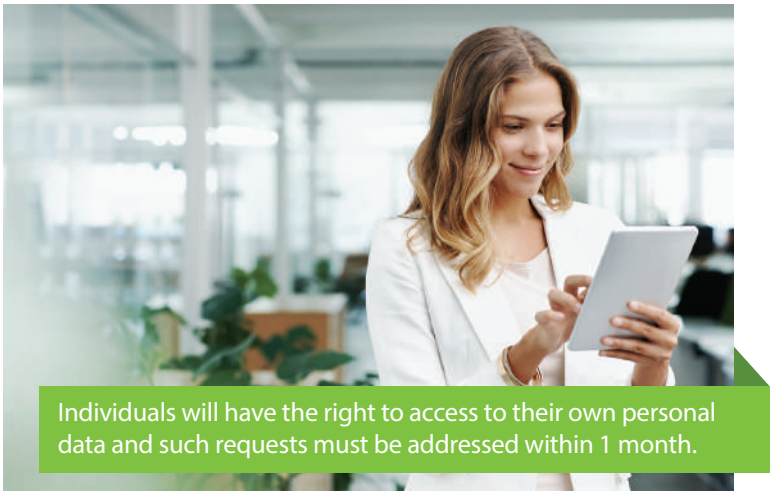
Here's an example of a more transparent privacy notice aimed at employees:

We are monitoring use of our broadcast email (intranet site, other internal vehicles) communications for the purpose of assessing content delivery, content and messaging format and length, device preferences, and for confirmation during critical corporate communication situations.

Information presented to employees must be written in consise, transparent , intelligable language that is easily accessible.

We may also use measurement analytics for our own legitimate business purposes, including campaign evaluation, messaging planning and internal training. We will retain individual email measurement data for no more than 90 days, unless such is being used to investigate an alleged crime or an incident, in which case it may be retained for up to two years following the conclusion of any investigation.
You have the following rights: request access to

email data relating to you, the rectification or erasure of your email interaction data of you (subject to other conditions), and the right to object to our use of email monitoring. Please contact our Privacy Officer, Mr. Smith, m.smith@xyz.com for any further information.



Individuals will have the right to access to their own personal data and such requests must be addressed within 1 month.

The GDPR gives data subjects certain rights, and controllers have the obligation to respond to a data subject's rightful inquiries within one month. Such rights include providing data subjects with access to any personal data processed, information regarding the source of the data, where the data is being processed, the purpose of such processing, and the period the data will be stored. Data subjects also have the right to request corrections and to request removal of data when it is no longer required for its original purpose. In addition, data subjects have the right to revoke consent, and consent "must be as easy to withdraw as it was to grant," according to Article 7(3).

Example 1: Performance Review

Let's make an example of the standard performance review. Any such file, including handwritten notes or digitally recorded comments, is considered personal information. The UK's Information Commissioner's office offers this by example:

"A manager's assessment or opinion of an employee's performance during their initial probationary period will, if held as data, be personal data about that individual. Similarly, if a manager notes that an employee must do remedial training, that note will, if held as data, be personal data."

Before any review, the employee must consent to having such opinions recorded, and must be made aware of who will have access to that data and what it will be used for. An organization must have a process in place whereby reviews are available to the employee, and can delete information once the employee leaves the organization.

Example 2: Web and Email Analytics

Corporations today routinely make use of web analytics and email analytics to understand their employees' use of communications and often leverage such data to improve the content and user experience. In many cases, these tools collect IP addresses and email addresses, allowing for individual actions to be identified. Therefore, employees must consent to the collection of such data, and employers must make clear the intent of such data processing, and not use the data for any other purpose. Consent for such automated data collection is difficult to obtain at the point of collection and is, therefore, best done by policy.

Employees must consent to the collection of private information embedded within company analytics reports.

Companies with citizens of the EU as employees should be reviewing and rewriting their consent policies now in preparation of the GDPR going into effect May 25, 2018. Ideally, this should not be left strictly to the legal team, as human resources and communications teams will have insights into particulars of the various employee programs and procedures which will be impacted by the new law. There is a lot at stake if your company is not in compliance.

What does the New EU Regulation mean to me?

According to a recent Forbes article, 96 percent of businesses with operations or employees in the UK, Germany, and France admit that they are underprepared for the General Data Protection Regulation (GDPR), despite the law becoming effective May 2018.

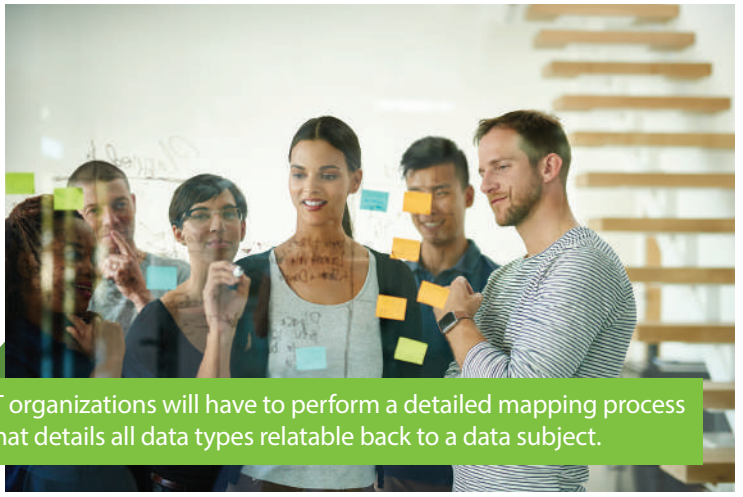
To comply with the GDPR, your organization will likely need a data protection officer, you will have to review and revise your employee agreements and any policies related to employee data, terms of use and privacy, and review your third-party vendor agreements along with their data security processing policies and procedures. It's important to note that the responsibility for compliance does not fall solely on the vendor – it's the primarily the business that shall be fined if using a software tool in violation of the new data privacy rules.

Most importantly, you will need to identify what personally identifiable information (PII) you have, how it gets processed and stored, and then educate your staff on the new requirements related to security and privacy.

When it comes to PII, the HR department is sitting on a treasure trove of names, addresses and phone numbers plus social and health insurance numbers, credit reports, payroll and bank account information – rich targets for hackers seeking valuable information for identity theft.

Depending on the size of your organization and the type of data it holds, it may be necessary to hire a Data Protection Officer.

GDPR compliance starts with awareness, and requires asking new questions regarding how and why data is received, processed and stored. Take stock of what data you collect, map how that data moves through your business process, and identify where it gets stored. Do you really need the data? For how long? Who has access to it? What protections are in place to secure it?



IT organizations will have to perform a detailed mapping process that details all data types relatable back to a data subject.

In "recognizing employee data privacy" we covered what constitutes personal data, and determined that EU employee information falls clearly into this category. In "Steps to Compliance" we highlighted the fact that the GDPR requires gaining consent from the data subject (for this discussion, your employee) for what data you are collecting, why and what you are doing with it, along with the requirement to protect it.

In many cases, you may find you are storing some personal data for no good reason, and can dispose of it once you are done with it. You may also discover that you can protect privacy and retain important bits of data at the same time.

Under GDPR, there are three broad categories of data:

- **Personal data.** Personal data is any information relating to an identified or identifiable natural person. An identifiable person is one who can be

identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

- **Anonymous data.** Anonymous data is any information from which the person to whom the data relates cannot be identified, whether by the company processing the data or by any other person.

- **Pseudonymous data.** Pseudonymization is a form of de-identification. Some sets of data can be amended in such a way that no individuals can be identified from those data (whether directly or indirectly) without a "key" that allows the data to be re-identified. A good example of pseudonymous data is coded data sets used in clinical trials.

The GDPR recognizes the privacy-enhancing effect of data anonymization by providing exceptions to many of the most burdensome provisions of the regulation when steps are taken to de-identify personal data. The GDPR also allows controllers and processors who pseudonymize personal data more leeway when it comes to processing the data for a purpose other than the one for which they were collected.

According to Germany's Federal Data Protection Act, "rendering anonymous" means "the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labor be attributed to an identified or identifiable individual."

Human Resources can get around measurement of internal email success by simply measuring results as anonymous.

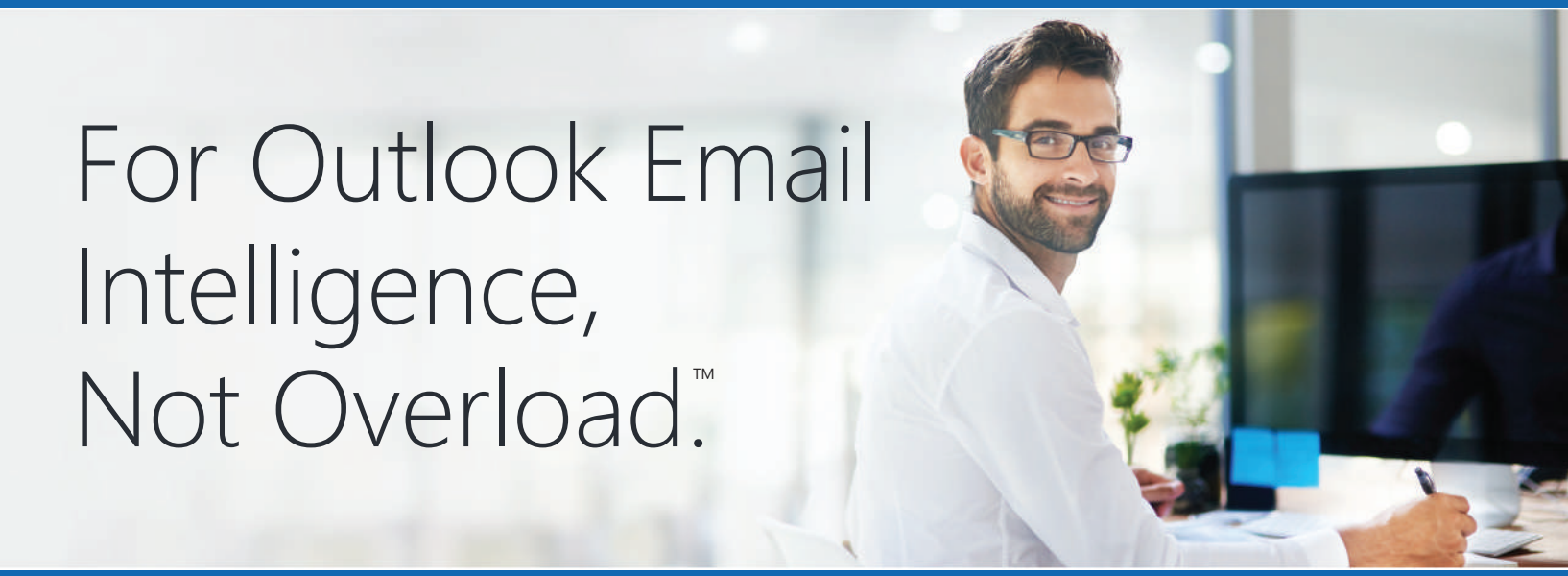
that is not perfectly anonymous, but sufficiently anonymous such that privacy is preserved without considerable technical time and expertise. In other words, if you cannot identify a person from the data (either directly or indirectly) then the GDPR rules shall not apply.

Additionally, the GDPR allows for pseudonymisation of data to satisfy the requirements of privacy, commonly referred to as "privacy by design." Using pseudonyms instead of personal data means one cannot identity a person (again, directly or indirectly) without a corresponding "key." An example might be encrypted data, or data for clinical trials in which the subject identity is coded. Such keys must be secured and kept separately from the data.

By making it impossible or impractical to connect personal data to an identifiable employee, companies are permitted to use, process and publish such information in just about any way that they choose. For many of your business processes, whether managed internally or by a third party, employing these techniques will make compliance much easier.

HR and communications leaders are often overloaded with rapidly changing demands, from educating and informing employees, onboarding new employees, managing benefits programs and participation, to encouraging and monitoring employee engagement. Adding the important responsibility of protecting the privacy of personal data related to employees, candidates and contractors might be easy to ignore or push off as a job for the IT or legal departments. But with GDPR, the rules of engagement with personal data have changed, and the biggest threat to compliance is your own employees access, use and potential inadvertent disclosure of such data. For those of us who work with employee PII every day, communication and education regarding the new responsibilities is the first step forward.

For Outlook Email Intelligence, Not Overload.™



PoliteMail offers three tracking modes, Aggregate, Individual and Anonymous. Aggregate Tracking and Individual/Anonymous Tracking are like apples and oranges. You are still tracking your total audience participation, but in very different ways. Aggregate mode tracks the email message, Individual and Anonymous modes tracks the recipients.

Anonymous Tracking

Anonymous Tracking collects name and email address information, but disassociates such PII from their email interactions. At the time of send, the tracking data is anonymized, such that PoliteMail users (even technically) are unable to determine if a specific person interacted with a specific message. This mode provides metrics as accurate percentages of your audience, but does not provide the ability to drill down to see any individual interaction behavior. Anonymous Tracking still allows personalization of the message (addressing by name). Use Anonymous Tracking to maintain individual employee privacy, as it is **compliant with the GDPR and other EU Data Privacy regulations.**

Find out more at http://www.politemail.com

PoliteMail Software
655 Portsmouth Avenue
Greenland, NH 03840
Toll-Free: 866 488-9768
sales@politemail.com
www.politemail.com

PoliteMail®
for Outlook Email Intelligence™