

NEW GDPR

EVERYTHING YOU NEED TO KNOW ABOUT
THE NEW DATA PROTECTION ACT



INDEX

Context	3
The need to protect information	4
A brief look at the new regulation	5
The new regulation	7
Does the GDPR apply to your organization?	9
Does the GDPR apply to your organization? - real cases	10
The price of infringement	11
New regulation checklist	12
What can I do?	15
The solution: Datapeers	16
The solution Datapeers: features	17
The solutions Datapeers: technical aspects	18
The solution Datapeers: operating scheme	19
Return on investment guaranteed	20
FAQ	21



CONTEXT

Companies face increasing data security and confidentiality threats, which forces them to reevaluate their data management strategies. All of us at some point in our lives conduct online actions, such as buying a product, subscribing to a service, or making a bank transfer. New technologies create a large number of opportunities for optimizing resources, but when are used in a wrong way, they can compromise the security of citizens' information.

One of the biggest concerns of all companies is the protection of private information. As never before the need to protect data was so evident. A study carried out by Forrester predicts that the global number of used smartphones will exceed 3.5 billion by 2020 and this massive use of mobile devices will power the existence of attacks, compromising in large measure the privacy of everyone.

Citizens must have control over their personal data and simplify the legal framework for digital business. For the European Commission, the protection of personal data is a key element of the Digital Single Market. All this scenario has boosted the creation of the new General Data Protection Regulation (GDPR) for the European Union, which repeals the current legislation on personal data protection, published in 1995, when Internet access was not yet widespread. The new regulation comes into force in May 2018.



THE NEED TO PROTECT INFORMATION

78%

of companies around the world have suffered at least one computer attack in the last two years

92%

of the attacks are due to internal security breaches

35%

of attacks are suffered due to information loss on mobile devices

57%

of companies doesn't protect information with data protection solutions.

61%

of loss of productivity in each computer attack

42%

of loss of revenue in each computer attack

3%

of companies has a plan to be implemented to ensure compliance with the GDPR in May 2018

4,8%

of companies are well aware of the new data protection regulation

44%

of companies admits that doesn't have a plan to comply with the GDPR on the date of its entry into force

A BRIEF LOOK AT THE NEW REGULATION



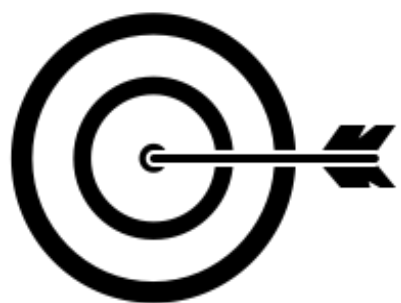
Official name

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data



Deadline

It takes effect on May 25, 2018



Purpose

It gives individuals in the European Union stronger rights by giving them greater control over their data and privacy in the digital age

A BRIEF LOOK AT THE NEW REGULATION



What is personal data?

According to the law, personal data means any information relating to an individual identified or identifiable through them (identifiable 'by reference to an identification number or to one or more specific elements of his physical, physiological, economic, cultural or social)



Certification

There is an optional certification for companies that successfully meet legal requirements. This certification can mean a competitive advantage and helps building customer confidence



THE NEW REGULATION

The legislative process on the new regulation started in 2012 in the European Commission and after some discussions reached the final version which was published in early May 2016. This new law applies in the 28 Member States of the European Union and enters into force on May 25, 2018.

The most significant and impacting changes in this new regulation are as follows:

- **Right to forget:** citizens will be able to require companies to delete their personal data. This right of forgetting is an extension of the existing right to prevent personal data being processed. The new regulation allows the personal data of each citizen to be destroyed.
- **Portability of data:** citizens may require companies to send their personal data in a format that allows them to be sent to another company, facilitating their migration and making it simpler to change service provision. Whenever a citizen changes a bank or a television service provider, he or she will not have to provide his or her personal data again as they can be easily migrated from one company to another.



THE NEW REGULATION

- **Right to oppose profiling:** companies' computer systems should be able to register who indicated a refusal to process their data automatically, as is usually done in behavioral analysis and profiling processes. In these situations, the records may not be included in the files.

- **Registrations and proof of consent:** in relation to online customer relations, company systems should expose privacy policies in clear and objective language. Consent to data processing by citizens should be retained to serve as evidence of free and unambiguous consent.

- **Privacy by 'defect' and design:** you should ensure the protection of data from the design of computer applications, minimizing the processing of personal data, data masking, encryption, among other aspects. The goal is to be able to explain the whole process of treatment and protection of data.

- **Obligation to notify:** companies and organizations have the duty to notify the National Supervisory Authority of data breaches for situations which put individuals at risk and to communicate to the citizen in question all high-risk violations as soon as possible, so that appropriate measures can be taken.



DOES THE GDPR APPLY TO YOUR ORGANIZATION?

The new data protection law applies to any organization doing business in the European Union, regardless of whether personal data processing occurs in the European Union or not, and regardless of whether it is personal data about EU residents or only visitors.

It is important to note that the new rules apply to companies established outside the European Union processing personal data of EU residents or visitors in connection with:

- Offers of goods or services, regardless of whether payment is required, or;
- Behavior Monitoring that occurs in the EU.

Having a website or an email accessible in the European Union is not enough to put the business under the umbrella of the new data protection regulation. However, some factors may indicate that an organization intends to offer goods or services to residents or visitors in the European Union, which brings the business into the scope of the new rules. These factors are:

- The use of a language or currency generally used in one or more Member States of the European Union with the possibility of ordering goods and services in that language;
- The mention of customers or users who are in the European Union.

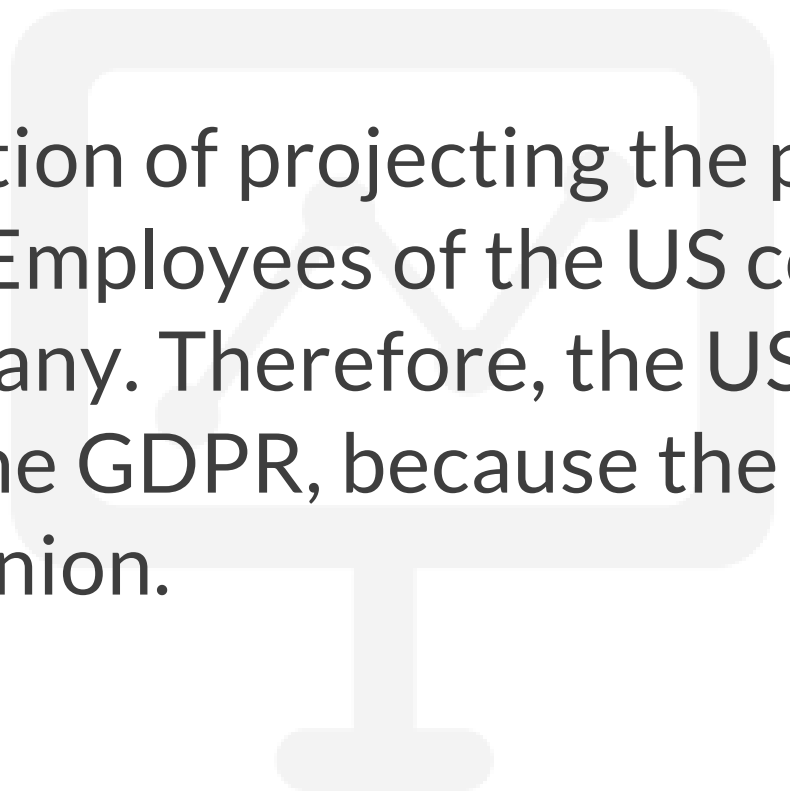


DOES THE GDPR APPLY TO YOUR ORGANIZATION?

Real Cases

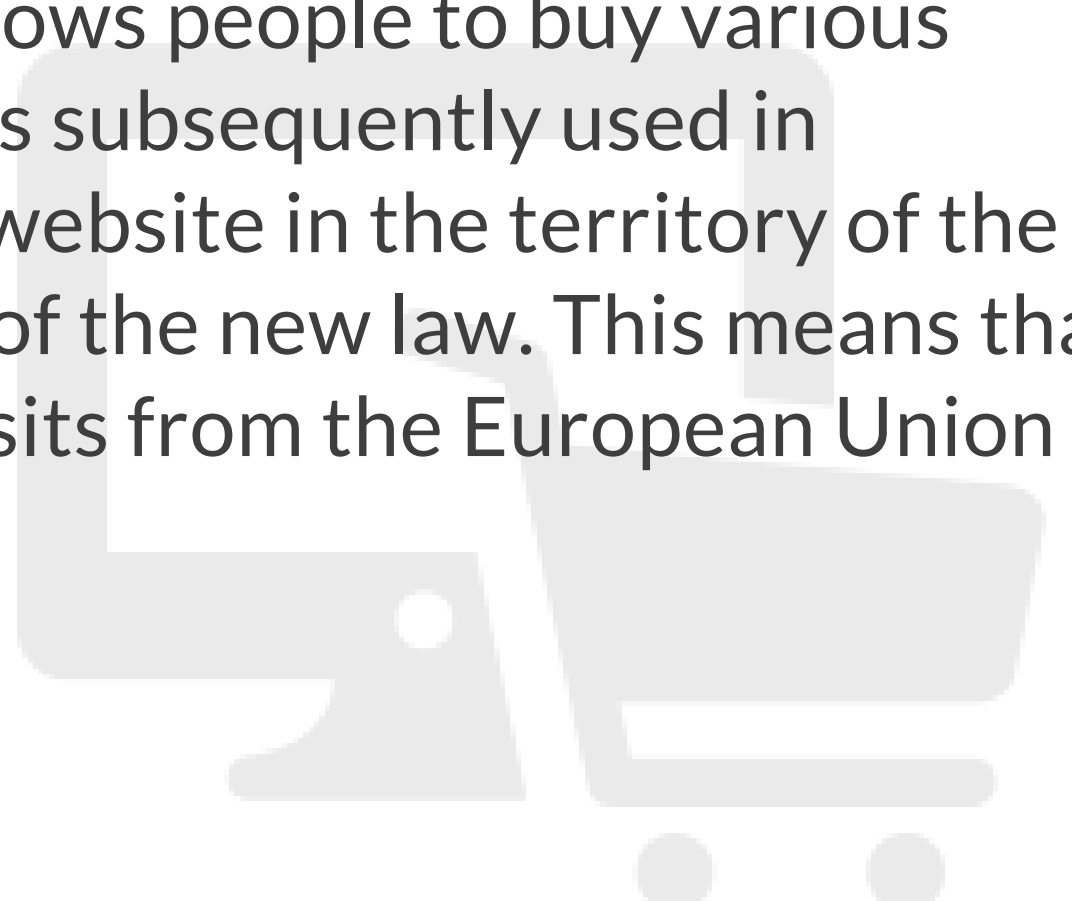
Scene 1

A company based in New York has the function of projecting the profits of a German company for the next three years. Employees of the US company will use data provided by the German company. Therefore, the US company is obliged to comply with the new rules of the GDPR, because the data were collected in the territory of the European Union.



Scene 2

"BuyEverything" is an American site that allows people to buy various products online. The site collects data that is subsequently used in marketing campaigns. If a person visits the website in the territory of the European Union, the site becomes "target" of the new law. This means that any website that collects data and allows visits from the European Union is obliged to comply with the new RGPD.





THE PRICE OF INFRINGEMENT

The infractions for those who don't comply with the new data protection law are quite heavy and are an important incentive to comply the law.

The minimum amount for fines has not been set, but penalties for breaches of personal data can reach 20 million euros or up to four percent of the company's annual worldwide turnover.

The fines may reach
€ 20,000,000.00 or, in the case of
a company, up to 4% of its annual
worldwide turnover
corresponding to the previous
financial year, whichever
is greater.



CHECKLIST OF THE NEW REGULATION



Inventory of personal data

Make a list of all the personal data with detailed information about the storage location. This will make it easier to have a comprehensive understanding of how personal data is stored in your company.



Analysis of data flow

Identify all systems that store personal data under the new GDPR. You must map the data streams from your point of entry to the time of destruction, including third-party processes. This data mapping will help you ensure that all risks of loss of personal data are eliminated (or at least widely minimized).

CHECKLIST OF THE NEW REGULATION



Registration of treatment activities

You should record in detail all activities related to the processing of personal data in order for the organization be able to demonstrate that it fulfills all the obligations in force in the GDPR. The legislation provides that subcontractors have almost the same obligations as those responsible for processing and are thus required to prove that they comply with what is required.



Identification of gaps

Define how you will correct the gaps detected during the risk assessment period. Prioritize problems according to the risk they present. The action plan for these situations may include: hiring new employees, training current employees, changing processes and methods, and implementing new technologies.



CHECKLIST OF THE NEW REGULATION



Risk assessment

Follow the contact points for data and do a risk assessment for each data source and storage location. In this way, you will be more prepared in case of attack and you will be able to identify and minimize the risks of suffering an attack and losing data.



Appointment of a Data Protection Officer

This figure plays an essential role in the transition period from the old law to the new legislation. The person responsible for data protection should ensure that everything is perfectly legal at the date of entry into force of the GDPR.



WHAT CAN I DO?

1

Analyze the personal data managed by the organization

- make an inventory of these data: type of data, where it was collected and where it is stored.

2

Check the privacy policy for the data collected

- verify that the privacy policies in the organization are clear and explicit, promoting the user's easy understanding.

3

Name a Data Protection Officer

- mandatory for companies with more than 250 employees or for companies that have third-party data processing or special category data (racial, ethnic, political, religious, among others) in their core business.

4

Implement data protection and management policies

-make sure that the location of personal data is known, that they are adequately protected from unauthorized access and that they are easily eliminated if you receive a request.

* We have a professional team able to assist you in this phase of transition to the new RGPD.
Contact us in case of doubt.

THE SOLUTION: DATAPEERS



DATA
INTEGRITY



DATA MASKING



TEST DATA
MANAGEMENT



TEST DATA GENERATION



DATA SUBSETTING

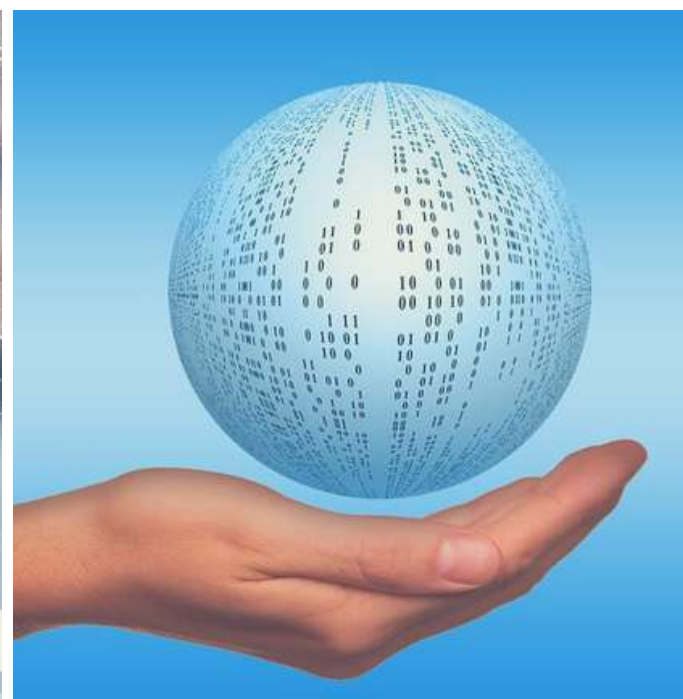


INTEROPERABILITY

Datapeers is an innovative and automated solution that enables data masking and helps companies meet data privacy requirements while enhancing the quality of software development, testing, training, and certification processes.

Datapeers is a complete solution that enables the automated creation of non-productive databases based on subsets of production data. In this way, it allows you to generate test data that meets the most demanding standards of software testing.

THE SOLUTION DATAPEERS Features



- ✓ Sophisticated masking techniques to protect sensitive data
- ✓ Automatic detection of data dependencies and hidden relationships
- ✓ Intelligent extraction of data subsets and creation of relevant data to different environments
- ✓ Meets the rules of confidential data protection

THE SOLUTION: DATAPEERS

Technical aspects



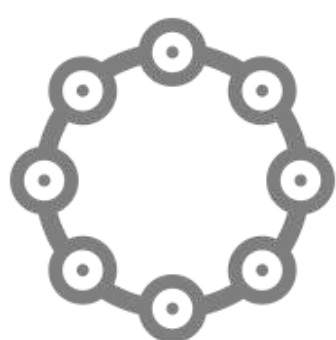
REFERENTIAL INTEGRITY

Consistent data relationships, ensuring data quality even after changes



DATA MASKING

Replacing actual data with fictitious but realistic data in accordance with the main corporate and government data protection rules and regulations



INTEROPERABILITY

Ability to work with multiple database technologies and operating systems



TEST DATA GENERATION

Data generator that allows programmers and administrators to populate databases automatically with meaningful and realistic test data

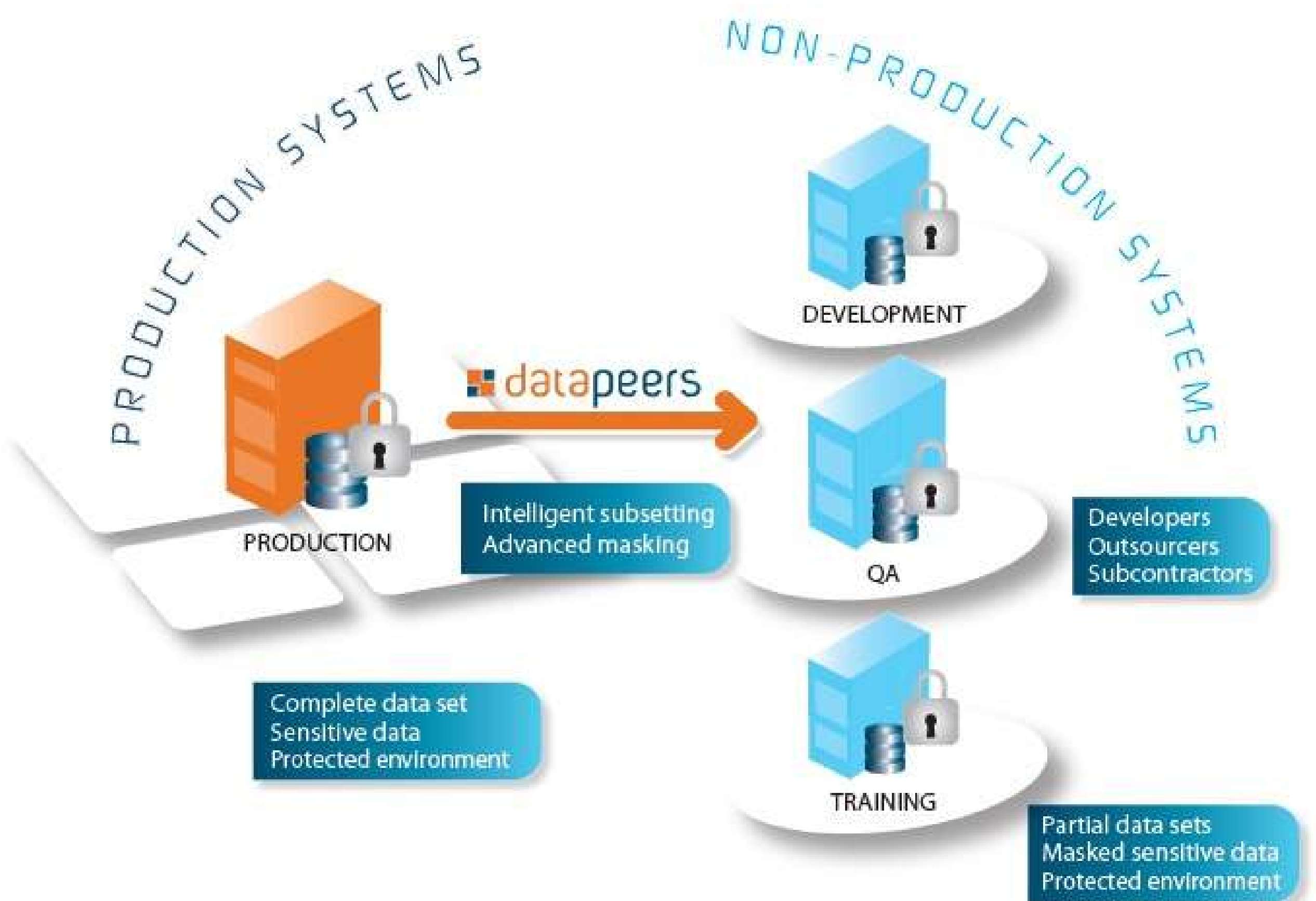


DATA SUBSETS

Multiple subsets of data that accurately reflect the original production database and meet the specific needs of each type of test

THE SOLUTION: DATAPEERS

Operating scheme



A pair of hands holding several gold coins, with a stack of coins in the center. The background is a blurred office setting.

RETURN ON INVESTMENT GUARANTEED

- ✓ **Increases team productivity** by up to 80% by automating most test data management tasks
- ✓ **Reduces testing costs** up to 75%
- ✓ **The test time** for new environments **is reduced by half**
- ✓ Increasing the quality of data **decreases the need to repeat tests** until the desired quality is achieved
- ✓ **Reduce infrastructure costs** by optimizing disk and server resources
- ✓ **Return on investment is achieved in less than six months** after the implementation of Datapeers

- ✓ **Ensures that non-productive environments meet GDPR obligations**



FAQ

Is it necessary to obtain consent from the data subject in the case of a database with public domain information (eg, professional number in the health sector)?

This issue is a paradigm, since the data related to the health sector are sensitive and it is recommended access only to the data strictly necessary for the continuation of the function of the collaborator. In these situations, in order to maintain the confidentiality and integrity of the data, you are advised to use a data masking tool, such as Datapeers.

What is Data Protection Impact Assessment (DPIA)?

According to the European Commission, the Data Privacy Impact Assessment (DPIA) is a process designed to describe private data processing, which assesses the need for processing and helps manage the risks related to the processing of personal data.

It is a risk assessment, which relates the impact of the realization of data privacy threats to their likelihood of occurring.




FAQ

What are the key changes to consent by individuals and businesses?

The Regulation creates additional barriers to current data collection and processing practices by introducing more stringent rules for companies with regard to consent for the collection and processing of personal data. Companies have to consider creating a contract with the data subject, complying with legal obligations and defending vital interests of the data owner. With the new regulation, a contact of a business card, for example, cannot be included in any database without the explicit consent of its owner. In practical terms, the use of previously selected boxes, the absence of responses, inactivity and consent through terms and conditions will no longer be allowed, as none of the means presented is considered a means of demonstrating compliance with the consent requirements of the new regulation.



**Talk to us and learn how we can help
you to meet the challenges of the new
GDPR**



***Before I write my
name on the board,
I'll need to know how
you're planning to
use my data.***

FOR MORE INFORMATION

**Centro Empresarial da Maia
Rua Eng. Frederico Ulrich, 3210
4470-605 Maia**

**www.datapeers.itpeers.com
info@itpeers.com
+351 220 101 587**