BIANCHI

GDPR

GDPR is "General Data Protection Regulation".

- Entry into force on 25 May 2018.
- Reinforces the protection of the individual's right to personal data protection, reflecting the nature of data protection as a fundamental right (diritto fondamentale) for the European Union.
- Guarantees the free flow of personal data between EU members States.

This is a new opportunity for companies and business. Why?

- A level-playing field (condizioni di parità) for all companies operating in the EU market.
- The principles of data protection by design and by default creating incentives for innovative solutions to address data protection issues form the start (protezione dei dati fin dalla loro creazione e incentive per soluzioni innovative).
- Stronger individuals' rights.
- More control over (riguardo) personal data for individuals.
- Stronger protection against data breaches (violazioni).
- The protection of the personal data guaranteed by the Regulation travels with the data outside the EU ensuring a high level of protection.

SUBJECT-MATTERS AND OBJECTIVE:

- This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
- This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
- The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Traduzione:

- Il presente regolamento reca norme relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e norme relative alla libera circolazione dei dati personali.
- Il presente regolamento tutela i diritti e le libertà fondamentali delle persone fisiche e in particolare il loro diritto alla protezione dei dati personali.
- La libera circolazione dei dati personali all'interno dell'Unione non è né limitata né vietata per motivi connessi alla tutela delle persone fisiche con riguardo al trattamento dei dati personali.

MATERIAL SCOPE:

- This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system (Il presente regolamento si applica al trattamento di dati personali effettuato, in tutto o in parte, con mezzi automatizzati e al trattamento non automatizzato di dati personali che fanno parte di un sistema di archiviazione o sono destinati a far parte di un sistema di archiviazione).
- This Regulation does not apply to the processing of personal data:
  (a) in the course of an activity which falls outside the scope of Union law;
  (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity; (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

TERRITORIAL SCOPE:

- This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
- This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
  (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union;
  (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
- This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

DEFINITIONS:

PERSONAL DATA: Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Examples of Personal Data:

- a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- an Internet Protocol (IP) address;
- a cookie ID;
- the advertising identifier of your phone;
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

Examples of Data not considered Personal Data:

- a company registration number;
- an email address such as info@company.com;
- anonymized data.

PROCESSING: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Examples of processing:

- staff management and payroll administration;
- access to/consultation of a contacts database containing personal data;
- sending promotional emails (to send direct marketing emails, you also have to comply with the marketing rules set out in the ePrivacy Directive);

- shredding documents containing personal data;
- posting/putting a photo of a person on a website;
- storing IP addresses;
- video recording.

PROFILING: Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

PSEUDONYMIZATION: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

FILING SYSTEM: Any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

CONTROLLER: The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

PROCESSOR: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

RECIPIENT: A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

CONSENT: Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

PERSONAL DATA BREACH: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

GENETIC DATA: Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

BIOMETRIC DATA: Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

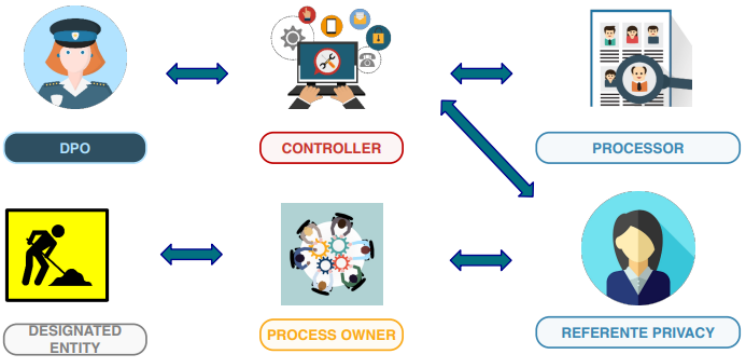
DATA CONCERNING HEALTH: Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

Who is the controller? The controller or processor may provide under their own responsibility and within the framework of the respective organisation that specific tasks and functions relating to the processing of personal data be allocated to expressly designated (indicate per lo svolgimento di un incarico) natural persons acting under the controller's or processor's authority ("Referente privacy"). The controller or processor shall set out the most appropriate arrangements to authorise the persons acting under their authority to process personal data ("Incaricato/Autorizzato al trattamento").

Who is the process owner? The person responsible for the process and the contact person for all information relating to the flows.

Who is the data protection officer? The person responsible for monitoring the compliance of the organization for which they work, giving advice and guidance relating to data protection obligations and acting as a contact point between data subjects and the relevant supervisory authority.



The controller needs to configure the data processing by providing, before proceeding with the processing, the essential guarantees to protect the rights of the interested parties, taking into account the overall cost and the risks for the interested parties. A preventive analysis and application commitment is required on the part of the controller, which must take the form of a series of specific and demonstrable activities. The most important activity is the Risk analysis, which detects the negative impacts of the processing on the freedoms and rights of the interested parties.

DATA PROTECTION BY DESING:

Taking into account the state of the art(the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing), the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

DATA PROTECTION BY DEFAULT:

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

The controller needs to configure the data processing by providing, before proceeding with the processing, the essential guarantees to protect the rights of the interested parties, taking into account the overall cost and the risks for the interested parties. A preventive analysis and application commitment is required on the part of the controller, which must take the form of a series of specific and demonstrable activities. The most important activity is the Risk analysis, which detects the negative impacts of the processing on the freedoms and rights of the interested parties.

RISKS FOR FREEDOM AND THE RIGHTS OF DATA SUBJECTS:

They may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of

their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

In general, technical and organizational measures and necessary safeguards can be understood in a broad sense as any method or means that a controller may employ in the processing. Being appropriate means that the measures and necessary safeguards should be suited to achieve the intended purpose, i.e. they must implement the data protection principles effectively. The requirement to appropriateness is thus closely related to the requirement of effectiveness. Effectiveness is at the heart of the concept of data protection by design. The requirement to implement the principles in an effective manner means that controllers must implement the necessary measures and safeguards to protect these principles, in order to secure the rights of data subjects. This observation has two consequences:

- First, it means that Art. 25 does not require the implementation of any specific technical and organizational measures, rather that the chosen measures and safeguards should be specific to the implementation of data protection principles into the particular processing in question. In doing so, the measures and safeguards should be designed to be robust and the controller should be able to implement further measures in order to scale to any increase in risk. Whether or not measures are effective will therefore depend on the context of the processing in question and an assessment of certain elements that should be taken into account when determining the means of processing.
- Second, controllers should be able to demonstrate that the principles have been maintained.

The implemented measures and safeguards should achieve the desired effect in terms of data protection, and the controller should have documentation of the implemented technical and organizational measures. To do so, the controller may determine appropriate key performance indicators (KPI) to demonstrate the effectiveness. A KPI is a measurable value chosen by the controller that demonstrates how effectively the controller achieves their data protection objective. KPIs may be quantitative, such as the percentage of false positives or false negatives, reduction of complaints, reduction of response time when data subjects exercise their rights; or qualitative, such as evaluations of performance, use of grading scales, or expert assessments. Alternatively to KPIs, controllers may be able to demonstrate the effective implementation of the principles by providing the rationale behind their assessment of the effectiveness of the chosen measures and safeguards.

The reference to “state of the art” imposes an obligation on controllers, when determining the appropriate technical and organisational measures, to take account of the current progress in technology that is available in the market. The requirement is for controllers to have knowledge of, and stay up to date on technological advances; how technology can present data protection risks or opportunities to the processing operation; and how to implement and update the measures and safeguards that secure effective implementation of the principles and rights of data subjects taking into account the evolving technological landscape.

The controller may take the *cost of implementation* into account when choosing and applying appropriate technical and organisational measures and necessary safeguards that effectively implement the principles in order to protect the rights of data subjects. The cost refers to resources in general, including time and human resources. Controllers must take into consideration the nature, scope, context and purpose of processing when determining needed measures. The concept of *nature* can be understood as the inherent characteristics of the processing. The *scope* refers to the size and range of the processing. The *context* relates to the circumstances of the processing, which may influence the expectations of the data subject, while the purpose pertains to the aims of the processing.

Data protection by design shall be implemented "at the time of determination of the means for processing" The "means for processing" range from the general to the detailed design elements of the processing, including the architecture, procedures, protocols, layout and appearance. The "time of determination of the means for processing" refers to the period of time when the controller is deciding how the processing will be conducted and the manner in which the processing will occur and the mechanisms which will be used to conduct such processing. It's in the process of making such decisions that the controller must assess the appropriate measures and safeguards to effectively implement the principles and rights of data subjects into the processing, and take into account elements such as the state of the art, cost of implementation, nature, scope, context and purpose, and risks. This includes the time of procuring and implementing data processing software, hardware, and services. Once the processing has started, the controller has a continued obligation to maintain DPbDD, i.e. the continued effective implementation of the principles in order to protect the rights, staying up to date on the state of the art, reassessing the level of risk, etc. The nature, scope and context of processing operations, as well as the risk may change over the course of processing, which means that the controller must re-evaluate their processing operations through regular reviews and assessments of the effectiveness of their chosen measures and safeguards.

The term "by default" when processing personal data, refers to making choices regarding configuration values or processing options that are set or prescribed in a processing system, such as a software application, service or device, or a manual processing procedure that affect the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

Personal data collected shall not be stored if it is not necessary for the purpose of the processing. The controller shall limit the retention period to what is necessary for the purpose. If personal data is no longer necessary for the purpose of the processing, then it shall by default be deleted or anonymized. The length of the period of retention will therefore depend on the purpose of the processing in question. This obligation is directly related to the principle of storage limitation and shall be implemented by default, i.e. the controller should have systematic procedures for data deletion or anonymization embedded in the processing.

PERIOD OF STORAGE ABOUT THE DATA:

Personal data collected shall not be stored if it is not necessary for the purpose of the processing. The controller shall limit the retention period to what is necessary for the purpose. If personal data is no longer necessary for the purpose of the processing, then it shall by default be deleted or anonymized. The length of the period of retention will therefore depend on the purpose of the processing in question. This obligation is directly related to the principle of storage limitation and shall be implemented by default, i.e. the controller should have systematic procedures for data deletion or anonymization embedded in the processing. Anonymization of personal data is an alternative to deletion, provided that all the relevant contextual elements are taken into account and the likelihood and severity of the risk, including the risk of reidentification, are regularly assessed.

ACCESSIBILITY:

The controller should limit who has access and which types of access to personal data based on an assessment of necessity, and also make sure that personal data is in fact accessible to those who need it when necessary, for example in critical situations. Access controls should be observed for the whole data flow during the processing. Personal data shall not be made accessible, without the individual's intervention, to an indefinite number of natural persons. The controller shall by default limit accessibility and give the data subject the possibility to intervene before publishing or otherwise making available personal data about the data subject to an indefinite number of natural persons. Making personal data available to an indefinite number of persons may result in even further dissemination of the data than initially intended. This is particularly relevant in the context of the Internet and search engines. This means that controllers should by default give data subjects an opportunity to intervene before personal data is made available on the open Internet. This is particularly important when it comes to children and vulnerable groups. Depending on the legal grounds for processing, the opportunity to intervene (accedere ai dati) could vary based on the context of the processing. Even in the event that personal data is made available publicly with the permission and

understanding of a data subject, it does not mean that any other controller with access to the personal data may freely process it themselves for their own purposes – they must have their own legal basis.

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

When a processing may have a high risk for the rights and freedoms of the data subjects, art. 35 GDPR obliges data controllers to carry out an assessment before starting it, consulting the supervisory authority if the technical and organizational measures used to mitigate the impact of the processing are not considered sufficient (that is, when the residual risk for the rights and freedoms of the interested parties remains high) ("prior consultation").

A Data Protection Impact Assessment (DPIA) is a systematic process that helps organizations identify and minimize the risks associated with processing personal data. The purpose of a DPIA is to assess the potential impact that a specific processing activity may have on individuals' privacy and data protection rights.

The main objectives of conducting a DPIA are:

- Risk identification: A DPIA helps identify and evaluate the risks and potential negative consequences that may arise from the processing of personal data.
- Risk mitigation: By identifying the risks, organizations can then determine appropriate measures to mitigate or minimize those risks.
- Compliance assurance: Conducting a DPIA is often a legal requirement under data protection regulations, such as the European Union's General Data Protection Regulation (GDPR).

WHEN DPIA IS MANDATORY?

In general, it is highly suggested to be done, but is mandatory in certain cases:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person; or
- processing on a large scale of special categories of data (referred to in Article 9(1)), or of personal data relating to criminal convictions and offences (condanne penali o reati)(referred to in Article 10); or
- a systematic monitoring of a publicly accessible area on a large scale.

WHEN PROCESSING MAY PRESENT RISKS TO THE RIGHTS AND FREEDOMS OF NATURAL PERSONS?

Working Party art. 29 (WP29) has identified some specific criteria:

- Evaluation or scoring, including profiling and predicting, especially from "aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements".
- Automated-decision making that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or "significantly affects the natural person" (for example, the processing may lead to the exclusion or discrimination against individuals).
- Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks. This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware (non sono consapevoli) of who is collecting their data and how they will be used.
- Sensitive data or data of a highly personal nature are managed: this includes special categories of personal data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10.

- Data processed on a large scale:

    - a. the number of data subjects concerned (either as a specific number or as a proportion of the relevant population);
    - b. the volume of data and/or the range of different data items being processed;
    - c. the duration, or permanence, of the data processing activity;
    - d. the geographical extent of the processing activity.

  (Note: the GDPR does not define what constitutes large-scale, but the WP29 recommends that these factors should be considered when determining whether the processing is carried out on a large scale).
- Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes.
- Data concerning vulnerable data subjects: because the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights.
  Vulnerable data subjects may include children, employees, people requiring special protection (mentally ill persons, patients, etc.), and in general, where there is an imbalance between the data subject and the controller.
- Innovative use or applying new technological, like combining use of finger print and face recognition for improved physical access control. The GDPR makes it clear that the use of a new technology, can trigger the need to carry out a DPIA. This is because the use of such technology (for example IoT devices) can involve new forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms.
- When the processing in itself "prevents data subjects from exercising a right or using a service or a contract" (for example a bank doesn't give a loan to a certain client).

WHEN ISN'T A DPIA REQUIRED?

When the processing is not "likely to result in a high risk", or a similar DPIA exists, or it has been authorized prior to May 2018, or it has a legal basis, or it is in the list of processing operations for which a DPIA is not required.

WP29 considers that a DPIA is not required in the following cases:

ripete le stesse cose

- where the processing is not "likely to result in a high risk to the rights and freedoms of natural persons";
- when the nature, scope, context and purposes of the processing are very similar to the processing for which DPIA have been carried out;
- when the processing operations have been checked by a supervisory authority before May 2018;
- where a processing operation has a legal basis in EU or Member State law, where the law regulates the specific processing operation and where a DPIA has already been carried out as part of the establishment of that legal basis;
- where the processing is included on the optional list (established by the supervisory authority) of processing operations for which no DPIA is required. In such cases, a DPIA is not required, but only if the processing strictly follows the "rules" and continues to comply them.

AT WHAT MOMENT SHOULD A DPIA BE CARRIED OUT?

Prior to the processing. This is consistent with data protection by design and by default principles. The DPIA should be seen as a tool for helping decision-making concerning the processing.

WHO IS OBLIGED TO CARRY OUT THE DPIA?

The controller, with the DPO and processors.

The controller is responsible for ensuring that the DPIA is carried out. Carrying out the DPIA may be done by someone else, inside or outside the organization, but the controller has the responsibility of it.

WHAT IS THE METHODOLOGY TO CARRY OUT A DPIA?

The GDPR sets out the minimum features of a DPIA:

- a description of the processing operations and the purposes of them;
- an assessment (valutazione) of the necessity and proportionality of the processing;

- an assessment of the risks to the rights and freedoms of data subjects;
- the measures envisaged (previste) to:
    - address the risks;
    - demonstrate compliance with this Regulation.

IS THERE AN OBLIGATION TO PUBLISH THE DPIA?

No, but publishing a summary could foster trust, and the full DPIA must be communicated to the supervisory authority in case of prior consultation or if requested by the DPA.

ORDER AGAINST FOODINHO S.R.L.

Foodinho was an Italian company which delivers, by way of a digital platform and through riders, food or other goods supplied by retailers following orders placed by customers.

The order by the Italian SA concerns the processing of riders' personal data.

INFRINGEMENTS REGARDING THE INFORMATION PROVIDED BY FOODINHO TO THE RIDERS

Some articles of the GDPR were infringed by Foodinho regarding the information provided to the riders:

- Article 5(1)(a): personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject.
    - Was infringed in respect of the transparency principle, in particular Foodinho failed to specify the following: the ways for processing location data, the generic information provided, the categories of collected data, in particular data regarding the conversations via chats, emails and/or phone calls with the call center, the evaluation of riders by customers.
    - Was infringed with regard to the fairness principle, since the obligation to inform employees as part of the employer-employee relations.

- Article 13(2)(a): in addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.
    - Was infringed since the information notice only provided inaccurate information on storage periods and it failed to specify the storage periods for certain data categories.

- Article 13(2)(f): in addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: (f) the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
    - Was infringed since the information notice didn't refer to any automated processing activities, including profiling, but such activities were found by Italian SA, in particular Foodinho was intended to score riders so as to rank them in terms of priority in booking the time slots. Additionally, no information was provided about the logic and consequences of such processing for data subjects.

- Article 13(1)(b): where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (b) the contact details of the data protection officer, where applicable.
    - Was infringed since no contact details for the DPO were provided.

VOLENDO SI POSSONO AGGIUNGERE GLI ARTICOLI COMPLETI MA NON CREDO SIA IMPORTANTE

INFRINGEMENTS REGARDING STORAGE PERIOD

- Article 5(1)(e): personal data shall be kept in a way such that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods only if they are used for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, but always respecting the "storage limitation", which is a regulation to safeguard the rights and freedoms of the data subject.

    - Was infringed since the company stores several categories of riders' data for all the duration of the employment relation as well as until 4 years following termination of employment.

in sostanza troppe informazioni raccolte e troppe persono che potevano verderle

INFRINGEMENTS REGARDING CONFIGURATION OF THE SYSTEMS RELIED UPON BY THE COMPANY

Article 5(1)(c) GDPR (data minimization principle) and Article 25 GDPR (privacy by design and by default principles) were infringed since the systems relied upon by the company were configured in a way to collect and store all the data relating to the handling of orders enabling to the authorized operators to use these data. In addition, the chat and email management system were configured to enable each operator to directly access the contents of the chats and emails exchanged with riders.

Of note, there was a huge number of entities that were authorised by the company to full access to riders' data, including detailed information.

INFRINGEMENTS REGARDING THE SECURITY MEASURES IN PLACE

Article 32 GDPR was infringed since the systems were configured from the start of the company's business in 2016, until at least activation of the so-called city permission so as to enable access by default to a lot of personal data by a huge number of system operators in connection with a wide number of tasks to be done by riders.

This did not allow ensuring "confidentiality, integrity, availability" permanently, which can have some consequences about the risks due to the "loss, alteration, unauthorized disclosure or accidental or illegal access to the personal data".

MANCA LA SLIDE 19 MA HO MESSO UNA CROCE SOPRA E NON DICE NIENTE DI INTERESSANTE

INFRINGEMENTS REGARDING AUTOMATED PROCESSING, INCLUDING PROFILING

Article 22 (Automated individual decision-making, including profiling):

The data subject shall have the right not to be subject to a decision based only on automated processing, including profiling, which produces legal effects concerning or which affects him or her.

This procedure is not applied if the decision:

(a) is necessary for entering into a contract between the data subject and a data controller;

(b) is authorized by Union or Member State law, to which the controller is subject;

(c) is based on the data subject's explicit consent.

- Was infringed since the company carried out automated processing activities, including profiling, both within the framework of the so-called 'excellence system' and as part of the order allocation system. The company didn't also implement suitable measures "to safeguard the data subject's rights and freedoms and legitimate interests".

INFRINGEMENTS REGARDING THE RECORDS OF PROCESSING ACTIVITIES

Article 30 (Records of processing activities):

Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.

That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients which will use the personal data, including recipients in third countries or international organizations;

(e) where applicable, transfers of personal data to a third country or an international organization, including their identification;

(f) where possible, the expiration time limits of the different categories of data;

(g) where possible, a general description of the technical and organizational security measures.

- Article 30(1), letters a), b), c), f), and g) was infringed since the records did not include: information on several categories of personal data, no specific information on storage periods, no general description of the technical and organizational security measures and, at the end, the records did not allow keeping track of their change history.

OUTCOME OF THE PROCEDURE

The Italian SA ordered the company to bring their processing operations into compliance with the GDPR in respect of the following:

- The documents containing the information notice, the records of processing operations and the DPIA, by also ensuring consistency among the processing operations;
- Specification of the storage periods of processed data;
- Suitable measures to safeguard the data subject's rights, fundamental freedoms and legitimate interests, at least the right to express his or her point of view and to contest the decision, with regard to the automated processing, including profiling;
- Suitable measures to regularly check fairness and accuracy of the results of algorithmic systems, in order to minimize the possible errors of the algorithm;
- Suitable measures to introduce arrangements (disposizioni) that can prevent inappropriate and/or discriminatory applications of feedback-based reputational mechanisms;
- Introduce arrangements to adopt the privacy by design and by default principles about the entities authorized to access to various data categories;
- An administrative fine of 2'600'000 €.

COOKIES CONSENT

APPLICABLE LEGISLATION

- Section 122 Italian DP Law
- Articles 4(11), 7, 12, 13 and 25 GDPR
- Italian Authority Guidelines on the use of cookies and other tracking tools

DEFINITIONS FOR LEGAL PURPOSE

Cookies:

- text strings that the websites (so called "publisher" or "first party" websites) visited by the user or web servers (so called "third parties") place and store, within a terminal device in the user's possession, directly as is the case with publisher websites, or indirectly as is the case with "third parties";
- software for browsing the internet and operating on devices which can store cookies and then transmit them back to the sites that generated them in order to keep track of that user's previous interaction with one or more websites.
  Information encoded in cookies may include personal data, such as an IP address, a username, a unique identifier or an email address, but it may also include non-personal data such as language settings or information on the type of device a person is using to navigate within the website;

- can perform diverse functions, including session monitoring, the storage of specific server access information related to user configuration, facilitating the use of online content, etc. For example, they can be used to keep track of the items in an online shopping basket or the information used to fill in a computer form. They are also used to allow web pages to upload more quickly information on a network or for advertising purpose such that advertisements can be customized for each particular user, based on its behavior on the network.

FIRST-PARTY AND THIRD-PARTY ANALYTICS COOKIES:

They can be considered as technical cookies if:

- They are only used to produce aggregated statistics concerning a single site or a single mobile app;
- At least the fourth component of each IP address is masked out (as for third-party cookies)
- The third parties do not match the analytics cookies data with any other information and do not forward such data to other third parties. However, statistical analyses that can be traced back to the same publisher are allowed.

OTHER TRACKING TOOLS:

Are tools that allow, more or less, to achieve the same objectives. They can be classed as: "active identifiers" (including cookies) or "passive identifiers" (which have just an observational role).

The 'passive' tools include fingerprinting, which a technology to identify the user's device by collecting all or part of the information on the specific configuration of a device. This technique can be used to achieve some profiling purposes, including the advertising and the offered services based on the user behavior.

For these reasons, fingerprinting and other tracking tools must be included in the scope of the Guidelines.

There is a significant difference between the use of an active technique, such as cookies, and a passive one, such as fingerprinting.

In the first case users who do not wish to be profiled are able to refuse their consent or can avail themselves of the rights provided for in the Regulation, but they have also the possibility of directly removing the cookies stored on their own devices.

In the second case, the user does not have tools on which he can rely to, independently, so he must rely the controller's support. The controller uses a reading technique that does not require the storage of information within the user's device, because, as we said before, these techniques have an observational role. The outcome is a "profile" of the user that remains in the controller's sole possession, to which the data subject has no free and direct access.

CATEGORIZATION OF COOKIES AND OTHER TRACKING TOOLS

Cookies and other tracking tools can have different features depending on their duration: they can be session or permanent cookies, or depending on the entity placing them, the publisher can act directly or on behalf of a 'third party'.

The legislation, provide two big categories:

- Technical cookies, which are used to establish a communication over an electronic communications network, so they are used for navigation and provide services to the users;

- Profiling cookies, which are used to create customized profiles, based on the users' activities, for the purpose of grouping the different profiles within homogeneous, multi-sized clusters; this allows the controller to provide customized services and also send targeted advertising messages.

SLIDE 14 NIENTE DI IMPORTANTE

AUTHORITY GUIDELINES

Guidelines takes into account:

- the legal framework of reference, especially the GDPR;

- rapid and continuous technical and technological innovation of networks and tools;
- the evolution of user behavior, with the consequent increment of the possibilities of collection data.

KEY POINTS

- Accountability (responsabilità)
- Expanded information obligations (data storage periods to be specified as well)
- Enhanced consent
- Compliance (conformità) with privacy by design and privacy by default principles
- Extension of the application of other tracking tools (i.e. fingerprint)

INFORMATION AND CONSENT

Information should be provided:

- By using simple, accessible language;
- In such a way as to be transmitted, without any discrimination, also to individuals needing assistive technologies or special configurations on account of their disabilities;
- Also by relying on multi-layered, multi-channel approaches;
- If only technical cookies are used, the relevant information may be placed on the website's homepage and/or in the general information notice.

If other cookies and non-technical identifiers are also used, a pop-up banner can be used including:

- A warning to the fact that the website uses technical cookies or profiling cookies or other tracking tools with relative information about the purposes (short information notice);
- A link to the privacy policy;
- A warning to the fact that if the banner is closed (e.g. by clicking on the 'X' on its top right corner) the default settings are left unchanged, so that the browsing can continue without cookies or other tracking tools other than technical ones.
- A button to accept all cookies or tracking tools;
- A link to an additional dedicated area where the user can select, individually, the functionalities and cookies that user consents to install, or withdraw his consents;
- In general, is a good practice using a graphical sign, an icon or any other flag (generally in the footer) to show the status of the consent declarations given by each user.

If the consent if denied, is not permitted to repeatedly ask for the consent, except if:

- one or more of the parameters of the processing changes significantly;
- it is impossible for the website to know if a cookie has already been stored on the device;
- at least six months have passed since the banner was last presented.

Regarding authenticated users (users having registered accounts), the data relating to their browsing on several devices may not be matched except with the users' consent.

EVALUATION OF METHODS TO OBTAIN CONSENT

Scrolling: this is a bit unsuitable to obtain valid consent, unless it allows the user to explicitly express his consent;

Cookie wall: this is unlawful, except where the website enables a user to access to the contents or services without consenting the installation and use of cookies (these situations must be seen case by case taking in account the GDPR principles).

VALIDITY OF EXISTING CONSENT

Pre-GDPR consent remains valid if it meets GDPR requirements and was recorded at the time it was obtained.