



## October 2019 EU affairs newsletter

---

Data protection .....	3
CJUE ruling on cookies consent .....	3
Finance .....	5
ESA’s priorities for 2020 .....	5
SME Finance .....	8
FEBIS takes part in SME Finance Forum in Amsterdam.....	8
European Data Protection Board.....	9
Italian New rules for credit reporting systems in the digital economy .....	9
Late payments.....	11
FEBIS takes part in the Late Payments reflexion workshop organised by the European Commission .....	11
Data & E-privacy.....	12
Data protection .....	13
CJEU rules that right to be forgotten applies only to EU individuals.....	13
EBA .....	13
EBA publishes Opinion proposing to further strengthen depositor protection in the EU .....	13
Data.....	13
Finnish Presidency platform on data in view of their high-level Expert conference end November .....	13
About FEBIS– Federation of Business Information Services.....	14





# Data protection

---

## CJUE ruling on cookies consent

On October 1<sup>st</sup>, 2019, the Court of Justice of the European Union issued a highly anticipated ruling on the scope of consent requirements with respect to cookie compliance. While the key points of the decision did not come as a big surprise to the privacy community, it will likely require many website operators to re-evaluate and update their cookie consent practices.

Importantly, with this [ruling](#), the CJEU established that consent cannot validly be obtained through the use of pre-checked boxes. The ruling resolves several specific questions about how consent can be validly obtained under the current EU data protection regime, including both the ePrivacy Directive and the EU General Data Protection Regulation.

### Background

The Federal Court of Justice in Germany, the Bundesgerichtshof, requested a preliminary ruling from the Court of Justice of the European Union regarding two questions on the meaning and application of Article 5(3) and Article 2(f) of Directive 2002/58/EC in conjunction with Article 2(h) of Directive 95/46/EC and Article 6(1)(a) of Regulation 2016/679.

The case involved participation in a lottery organized by Planet49 GmbH, an online gaming company. To enter the lottery, internet users were prompted to enter their postal codes, names and addresses, then presented with two checkboxes accompanied by explanatory texts. The first checkbox required the user to agree to be contacted by other firms for promotional offers. The second checkbox, which contained a pre-selected tick, required the user to consent to the installation of cookies on their device. In order to participate in the lottery, the first checkbox needed to be ticked.

The questions referred to the CJEU concerned consent, namely, whether valid consent had been obtained for storing information and for storing cookies on a user's terminal equipped if it has been sought "by way of a pre-checked checkbox which the user must unselect to refuse his consent." The CJEU was also asked to clarify whether information service providers need to give users information specifically about the duration of the operation of the cookies and whether third parties are given access to them.

### Key points

- **Consent must be obtained through active behavior**



Reading the consent provisions under Directive 95/46 and Regulation 2016/679 as requiring consent to be obtained through some active behavior on the part of the user, **the CJEU decided that a pre-ticked box does not constitute valid consent by the data subject.**

As the wording of Article 5(3) of Directive 2002/58/EC is that the user must have “given his or her consent” to the storage of and access to cookies on their terminal equipment, the court conceded that it “does not ... indicate the way in which that consent must be given.” However, regarding the phrase “given his or her consent,” the court argued that it “lend[s] itself to a literal interpretation according to which action is required on the part of the user in order to give his or her consent.”

Article 2(h) of Directive 95/46 defines “data subject’s consent” as “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.” Within this definition, the CJEU’s opinion and judgment focused on the term “indication,” which it argued, “clearly points to active, rather than passive, behaviour.” The court also noted that the consent is even more stringently defined under the GDPR and that the notion of “[a]ctive consent is thus now expressly laid down in Regulation 2016/679.”

Accordingly, if a user’s designation of consent is pre-formulated, the user is not giving active consent. As the advocate general stated, and as acknowledged in the CJEU’s judgment, “requiring a user to positively untick a box and therefore become active if he does not consent to the installation of cookies does not satisfy the criterion of active consent. ... By contrast, requiring a user to tick a box makes such an assertion far more probable.” Indeed, Recital 32 of the GDPR lists “ticking a box when visiting an internet website” as an example of how valid consent can be obtained from a user.

**Moreover, in his opinion, the advocate general also linked the notion of active consent to that of separate consent.** While the court’s judgment did not include this, he argued that it “appears ... doubtful” that bundling an expression of consent with the expression of another intention would be in conformity with the notion of consent under Directive 95/46.

- **Consent requirements also apply to the processing and storage of information that is not personal data**

As the CJEU noted, Article 5(3) of Directive 2002/58 (*eprivacy directive*) refers to the “storing of information, or the gaining of access to information already stored,” so **any such information would have privacy implications regardless of whether or not it constituted personal data within the meaning of Article 4(1) of the GDPR.** Recitals 24 and 25, as well as opinions of the Article 29 Working Party, corroborate this view that the information need not be personal data for Article 5(3) of Directive 2002/58 to apply.



- **Users must be provided information on cookie duration and access by third parties**

Finally, regarding the question of what information the service provider must give to provide clear and comprehensive information to the user in accordance with Article 5(3) of Directive 2002/58, the court ruled that this includes **the duration of the cookies and if third parties have access to them.**

- **Unresolved issues**

While it provided much-needed clarity on the more technical components of valid consent, it left open question as to whether the requirement for consent to be “freely given” (under Article 2(h) of Directive 95/46 and of Article 4(11) and Article 7(4) of Regulation 2016/679) is compatible with requiring a user to consent to the processing of their personal data for advertising purposes as a prerequisite for participation in a promotional lottery.

A judgment on this point would have brought much-needed clarity to the unresolved problem of so-called “cookie walls.” The choice to condition entrance to a website on the acceptance of cookies remains troublesome given the divergence of opinion among national data protection authorities on the issue. Although several DPAs (France, Germany, the Netherlands) have considered cookie walls not to be allowable under the GDPR, at least one — the U.K. Information Commissioner's Office — appears to be “sitting on the fence on this — at least for the moment.”

Consent is a critical topic that both lawmakers and privacy professionals continue to work toward better regulating, as well as implementing in practice. As pre-ticked boxes will likely fade into historical memory, more questions will undoubtedly arise about whether specific consent mechanisms are valid under the EU's data protection regime. **While the judgment demonstrates that consent must be obtained by “active” behavior, it will be interesting to see how website mechanisms change to meet this newly clarified standard.**

## Finance

---

### ESA's priorities for 2020

The Joint Committee of the European Supervisory Authorities (EBA, EIOPA and ESMA) published on October 2<sup>nd</sup> its 2020 Work Programme.

In 2020, under the EBA's chairmanship EBA, the Joint Committee of the three ESAs will continue its work in the areas of cross-sectoral risk analysis, consumer protection, financial conglomerates, securitisation as well as accounting and auditing.



Areas of particular focus of its work will be on PRIIPs, financial innovation - also in relation to the European Commission's FinTech Action plan and the work of the European Forum for Innovation Facilitators (EFIF) - as well as sustainable finance and securitisation.

Link to the 2020 programme : <https://eba.europa.eu/documents/10180/2970032/JC+2019+51+%28Joint+Committee+Work+Programme+2020%29.pdf>

Some issues that have been highlighted:

Topic/Activity	Artificial Intelligence
<b>Description</b>	The three ESAs will assess the phenomenon, focusing on potential consumer protection concerns and benefits associated to it.
<b>Expected Output</b>	Assessment of the Fintech phenomenon chosen; assessment of its benefits and risks; and, potentially, identification of any regulatory and/or supervisory measures which may need to be taken, taking into account the on-going sectorial work that the ESAs are doing in this field.

Topic/Activity	Use of behavioural finance findings for supervisory purposes
<b>Description</b>	In light of potential consumer protection concerns and benefits, the three ESAs will assess the use of insights from behavioural finance when dealing with existing and potential clients, especially when providing or collecting
<b>Expected Output</b>	Joint Report

Topic/Activity	Cross-sectoral risk analysis
<b>Description</b>	The ESAs will analyse the key trends and vulnerabilities to financial stability by using a comprehensive and cross-sectoral approach , which will be submitted to the to the Council's Economic and Financial Committee's Financial Stability Table for the spring and autumn meeting, and published.
<b>Expected Output</b>	Semi-annual Joint Report on Risks and Vulnerabilities.



Topic/Activity	Expected work 2020
<b>Joint Consumer Protection Day 2020</b>	In 2020, the ESAs will organise the 8th Joint Consumer Protection Day. Since its inception, the Consumer Protection Day has become an important milestone for stakeholders across the EU that have an interest in the topic of consumer protection.
<b>Cybersecurity / Technology area (includes cloud computing) / Joint work following FinTech Action Plan responses</b>	The ESAs will continue to work together particularly on the areas identified in the ESAs joint advices on legislative improvements relating to ICT risk management requirements in the EU financial sector (available here) and on cost benefit analysis of threat led penetration testing frameworks (available here), along with the Commission, to ensure alignment and a coordinated approach for cross-sector issues.
<b>Performance of retail investment products</b>	After the initial report on cost and performance, the ESAs will continue to discuss progress on the work regarding fees and the long-term performance of retail investment products at Joint Committee level.
<b>Brexit</b>	Continued discussion and coordination on any cross-sectoral issue coming as repercussion of the UK decision leaving the EU.

## EBA work programme for 2020

The European Banking Authority (EBA) published its detailed annual work programme for 2020, describing the specific activities and tasks of the Authority for the coming year and highlighting the key strategic areas of work for 2020.

In 2020, the EBA will focus on six strategic areas: (i) Support the development of the risk reduction package and the implementation of the global standards in the EU; (ii) Providing efficient methodologies and tools for supervisory convergence and stress testing; (iii) Moving towards an integrated EU data hub and a streamlined reporting framework; (iv) Making AML a real priority for the EU; (v) Contributing to the sound development of financial innovation and sustainability; (vi) Promoting an operational framework for resolution.

For more information :

<https://eba.europa.eu/documents/10180/2970032/EBA+2020+Work+Programme.pdf>



## SME Finance

---

### FEBIS takes part in SME Finance Forum in Amsterdam

As a response to the kind invitation from our industry partner, Sme finance forum, that highly contributed to the good cause of our last Febis event, we joined their last event in Amsterdam.

Over 600 people from 46 countries, representing the financing system. innovators from fintech, banks, software companies etc, have gathered together in this, mandatory to attend, platform to check the status of the new banking-fintech industry.

Some take -aways :

- \* The “credit rationing” (financial gap) has to be covered by a number of new innovative players.
- \* ecommerce and payment platforms entering the banking space.
- \* Fintechs are applying new technologies in their solutions have a new whole range of products available.

Some business models, could only apply to certain jurisdictions as, Asian and Latam regions, as data and license permissions (as well as financial systems) vary from region to region, or among countries.

- \* They are, also, using data in multiple ways. In our jurisdictions, we “only” need to balance this with legislation initiatives that hinder some uses and therefore, hinder the good cause of fintech.
- \* Many institutions as the OECD and the WORLD RESOURCES INSTITUTE (WRI) are working on this matter trying to light policy makers in their journey to set appropriate and fair rules for stakeholders.
- \* Febis will always be there, we met these 2 institutions, OECD and WRI, to open discussions for cooperation with our experiences and arguments.

The granularity of information is essential for running good credit assessments, that was stated in data governance and digital lending panels. Data protection/ownership/human rights have to balance with responsible use of data and legal frameworks. The concept is to embrace disruption. In Asia and Latam regions, many merchants are only willing to operate via fintech and known payment platforms.





Emerging countries are involved, in many aspects, within fintech and thus, become good innovators, however in EU jurisdictions some business models are not suitable due to legal constraints and different financial habits.

Together with, our industry partner, SME finance forum + the two new contacts, OECD and WRI, Febis will surely be in a better position to keep our trajectory to make our voice louder.

## European Data Protection Board

---

### Italian New rules for credit reporting systems in the digital economy

The main novelties for consumer credit, loans and new types of financing

Greater safeguards for consumers registered in credit databases, transparency on the functioning of algorithms that analyse financial risk, openness to new technologies and fintech services.

These are some of the innovations laid down in the new 'Code of conduct for credit reporting systems operated by private entities regarding consumer credit, creditworthiness and punctuality in payments', proposed by the trade associations and approved by the Italian Garante after a complex review of the old Code of Ethics, which has been rendered obsolete by the changes introduced by the European and national legislation on privacy.

The new rules for credit risk analysis — in order to adapt to the challenges posed by the digital economy — do not only concern data on loans and mortgages, but also those relating to different forms of leasing, long-term rental and the most innovative forms of loan between private entities ('peer-to-peer lending') managed through fintech platforms.

In order to facilitate the proper functioning of the financial and credit market, the records may be processed without the data subjects' consent, on the basis of the so-called legitimate interest of the companies participating in the credit reporting systems, while guaranteeing the wider rights set out in the European Data Protection Regulation. Only necessary, relevant data not exceeding the credit risk assessment purposes may be processed, by providing complete and timely information to the data subjects. For example, if you apply for a mortgage and your application is rejected, you will be able to know if the decision was taken also on the basis of the risk scoring given to you by an algorithm and, if so, to request to know the underlying logic.



In addition, the statistical analysis models as well as the algorithms used should be reviewed and updated at least every two years. Particular attention has been given to the security measures taken to protect the data from unlawful access and to ensure reliability of the systems. New forms of contact, such as those enabled by instant messaging systems used on smartphones, have also been identified in order to simplify the arrangements for informing data subjects prior to their registration in a credit reporting system (prior notice).

Some of the main novelties are listed below

- Rights: enhanced rights to protect the privacy of data subjects
- Disclosure: more complete information about the data processed by the participating companies
- Monitoring body: an independent body must be established to oversee the work of credit reporting systems
- New forms of contact: subject to agreement with the data subjects, 'alert notices' may also be sent by means of instant messaging systems that ensure traceability of the delivery.
- New credit categories: the scope of registered data was extended to include various forms of leasing, hire, lending between private parties (peer to peer lending)
- Longer positive data series: positive historical data on clients may be stored for 60 months to protect credit and to meet the demand coming from supervisory bodies
- Transparency in decisions: in the event of a denial of credit based on automated analysis, the data subject may request to know the logic underlying operation of algorithms
- Pseudonymised data for the training of algorithms: algorithms may be 'trained' with pseudonymised data, i.e. data that can no longer be related to a specific entity
- Security: additional measures are envisaged to protect data security and against unlawful access

In the approval decision, the Italian Garante nevertheless required credit reporting systems to make some changes to the functioning of the monitoring body established by the Code in order to strengthen its independence and autonomy from sector-related companies.

The members of the new Code of Conduct have committed themselves to comply forthwith with the rules and principles, even if the text will become fully effective only upon completion of the accreditation procedure of the monitoring body which requires the favourable opinion the EU Data Protection Board (EDPB).



## Late payments

---

### FEBIS takes part in the Late Payments reflexion workshop organised by the European Commission

On 21<sup>st</sup> October 2019, Nathalie Gianese and Stephanie Verilhac represented FEBIS at the Late Payments reflexion workshop organised by DG GROW of the European Commission to discuss the implementation of the late payment directive and the next steps.

The workshop began by a presentation from the European Commission about their findings on a study they made in 2018 on the implementation gaps of the Late payments directive. The presentation- which is available on request through FEBIS regulatory committee ( email Stéphanie at [stephanie@svmconsult.com](mailto:stephanie@svmconsult.com))- found out that

- only 39% respect agreed payments terms
- Excessive payment delays are suffered by more than 50% of companies, the majority being SMEs- payments delays over 60 Days;
- 70% do not claim interest or compensations out of fear factor , fear to ruin business relations.
- There has been a general reduction of 10 days, more results in PA2B brought back to 100 Days
- In some sectors, late payments still account for 1/3 of insolvencies and overall for ¼ of insolvencies

The key gaps put forward by the European Commission presentation are

- Legal loopholes : no maximum payment deadlines in B2B transactions
- Lack of provisions to support enforcement
  - o Lack of monitoring systems, not obligation to measure & report
  - o No enforcement bodies
  - o No rules clarifying grossly unfair terms
  - o No systems to manage complaints confidentially
- Lack of dedicated support to SMEs
  - o Training of credit management and lack of awareness about the directive
  - o Lack of affordable ADR procedures and cross-border resolutions

After the EC presentation, the workshop was organized around discussions under 3 major themes : enforcement, education& ethics and public bodies.

The first working site on enforcement concentrated on the different perceptions between representatives of big companies who do not wish to change the current Late Payment directive but put focus on enforcement, while the SME and sector representatives are claiming for a 30 days maximum payment delay and for some strict enforcement and fine rules.



FEBIS did a presentation during the second working site on education and ethics, where we insisted on what business reporting and credit scoring was and how it could help businesses with early warning processes before they get into liquidation phases provided business information providers can get access to relevant, updated and accurate information. The whole presentation was well received and was good to explain the sector and business model and avoid misconceptions like for example the confusion between rating and scoring. The whole workshop then went on about what was needed to provide better financial management skills to companies and entrepreneurs who often lack them.

The third workshop concentrated on public bodies and what some have done to improve payment delays by public administrations. For example the Netherlands explained that they now regulated a maximum period of 60 days for payment, more than that only if agreed and doesn't harm the smaller party. Act Payment deadline in 60 days came into force in 2017. In case of an agreement, when large party is buyer and small one supplier, cannot go over 60 days. After 2 years into force and the reflexion on enforcement, the general payment of invoice had shortened to 39.2 days.

At the end of the meeting, FEBIS provided the European Commission with a position paper explaining who FEBIS is, who are its members and what are the products and the clients FEBIS members have, and how it can be helpful to involve business information providers in the loop to help fight late payments.

## Data & E-privacy

---

The Federal Administrative Court in Leipzig has asked the Court of Justice of the European Union to clarify if the ePrivacy Directive supersedes the data retention provisions outlined in Germany's Telecommunications Act. Plaintiffs from two separate cases have objected to the obligation placed on them by both laws to store telecommunications data of their customers in reserve. A lower court ruled the plaintiffs are not required to store the data per the TKG. The lower court said the storage requirement infringes EU law and is not applicable to the plaintiff's cases. The appeal proceedings are on hold until the CJEU clarifies the rule.



## Data protection

---

### [CJEU rules that right to be forgotten applies only to EU individuals](#)

The Court of Justice of the European Union ruled the right to be forgotten can only be applied to individuals within the EU, The New York Times reports. The court determined the RTBF “is not an absolute right.” In a separate ruling, the CJEU said companies must consider free expression of information before deleting links with certain types of personal data. “The balance between right to privacy and protection of personal data, on the one hand, and the freedom of information of internet users, on the other, is likely to vary significantly around the world,” the court said in its decision. The [Times also reported](#) on a RTBF case involving an Italian journalist.

## EBA

---

### [EBA publishes Opinion proposing to further strengthen depositor protection in the EU](#)

The European Banking Authority (EBA) published its second opinion addressed to the EU Commission on the implementation of the Deposit Guarantee Schemes Directive (DGSD) in the EU. The Opinion focuses on the payouts by deposit guarantee schemes (DGSs) and proposes a number of changes to the EU legal framework, aimed at strengthening depositor protection, improving depositor information, enhancing financial stability and reinforcing operational effectiveness of DGSs.

## Data

---

### [Finnish Presidency platform on data in view of their high-level Expert conference end November](#)

Finland’s Presidency of the Council of the European Union runs from 1 July to 31 December 2019. They have identified the data economy as one of the strategic focus areas during Finland’s Presidency.



At the High-Level Conference on the Data Economy, to be held in Helsinki, Finland (25 to 26 November 2019), they will release the Presidency conclusions on the data economy and provide recommendations on horizontal principles for a European data economy.

The aim of this open website <https://dataprinciples2019.fi/about/> is to provide information on data economy principles and encourage open discussions about these principles.

[Read more here \(pdf\)](#)

The Finnish Presidency has flagged out 6 core principles on which open discussion can take place :

- **Access : Access by default.** Access to data according to various access rights (e.g. business-to-business, business-to-government) should be facilitated by technical or legal solutions and support.
- **Share : Reusable by default.** Data sets need to be interoperable and harmonised in a structured format to enable flow of data in automated processes.
- **Act : Human-centric by default.** Individuals are guaranteed access to their personal data and means to manage the reuse of their data without lockins or impediments that inhibit access or portability (e.g. timeliness).
- **Innovate : Level-playing field by default.** Data market access should be open to all on fair and non-discriminatory basis for the benefit of everyone. Undistorted competition in data markets should be guaranteed.
- **Trust : Ethically sustainable by default.** Building trust in data use and datadriven technologies requires strong respect for human rights, and transparency, reliability and the inclusion of all stakeholders. Data security and privacy by design should be integral parts of business and service development practices.
- **Learn : Renewal by default.** A thriving data economy requires societal change and constant re-evaluation and up-scaling of people's skills and organisational capabilities.

After the principles have been released at the conference, they are taken together with policy recommendations for further discussions at the Telecommunications Council in December 2019.



## About FEBIS– Federation of Business Information Services

Benefiting from the opening of markets within Europe and overseas, world-wide business has experienced substantial growth. As business grows so does the demand for business information intelligence for cross-border business activities.

In 1973, leading European credit information agencies joined forces to form the Federation of Business Information Services FEBIS (initially known as FECRO), with its registered office in Frankfurt. Today, FEBIS has developed into a sizable organization comprising more than 100 members from all over the world involved in providing Business Information and credit information services of national and International importance.

As the industry association, FEBIS strives to look after common interests of its members. While monitoring new legislation like data protection laws and insolvency laws, FEBIS also oversees and the application of public sources and information.