FIVERS

Regulatory update
Data protection, AI, IT and IP

n. 12 / 2024

DATA PROTECTION

9 October 2024 - European Data Protection Board: Guidelines on the processing of personal data based on legitimate interest.

---

9 October 2024 - European Data Protection Board: Opinion on Article 28 of the GDPR and on certain obligations arising from the designation of the External Data Processor (and sub-processors) adopted.

---

9 October 2024 – European Data Protection Board: the right to erasure ('right to be forgotten') shall be the topic for the fourth Coordinated Enforcement Action (CEF).

---

4 October 2024 – EU Court of Justice: an online social network such as Facebook cannot use all of the personal data obtained for the purposes of targeted advertising, without restriction as to time and without distinction as to type of data.

---

4 October 2024 – EU Court of Justice: Member States may make provision for competitors of the person allegedly responsible for an infringement of the laws protecting personal data to challenge that infringement in court as a prohibited unfair commercial practice.

---

4 October 2024 - EU Court of Justice: the limits of legitimate interest as a basis for the lawfulness of processing for marketing and commercial purposes.

---

4 October 2024 - EU Court of Justice: conditions for exercising the right to delete personal data from the Business Register held by a Member State and for claiming compensation for non-material damage in the event of a refusal.

---

4 October 2024 - CJEU publishes judgment on compensation for non-pecuniary damages under the GDPR.

ARTIFICIAL INTELLIGENCE.

14 October 2024 - EU Council: Directive on digital platform workers finally approved.

---

11 October 2024 – G7 Data Protection Authorities: the role of DPAs in regulating Artificial Intelligence.

DIGITAL MARKETS

10 October 2024 - Legislative decree 144/2024 for the harmonisation of national legislation with the provisions of Regulation (EU) 2022/868 on European data governance published in the Official Gazette.

---

10 October 2024 - EU Council: Cyber Resilience Act (CRA) definitively approved, introducing new security requirements for digital products.

---

9 October 2024 - European Banking Authority: Guidelines for issuers of asset reference tokens (ARTs) and electronic money tokens (EMTs) to ensure orderly and timely redemption of tokens in the event of an issuer's inability to fulfil its obligations.

INFORMATION TECHNOLOGY

8 October 2024 – Internal Revenue Agency: provision no. 379575/2024 on the procedures for communicating, changing and revoking data relating to the special digital domicile and for confirming or revoking the PEC address

---

2 October 2024 - Legislative Decree No. 138/2024, transposing Directive (EU) 2022/2555 - NIS 2 on a common level of cybersecurity in the EU, will enter into force on 16 October.

INTELLECTUAL PROPERTY

10 October 2024 - The IP measures in the Omnibus Decree, converted into Law 143/2024.

DATA PROTECTION

9 October 2024 - European Data Protection Board: Guidelines on the processing of personal data based on legitimate interest.

The EDPB adopted the Guidelines on the processing of personal data based on legitimate interest.

Data controllers need a legal basis to process personal data lawfully. Legitimate interest is one of the six possible legal bases.

These Guidelines analyse the criteria set down in Art. 6(1) (f) GDPR that controllers must meet to lawfully process personal data on the basis of legitimate interest. It also takes into consideration the recent ECJ ruling on this matter (C-621/22, 4 October 2024).

In order to rely on legitimate interest, the controller needs to fulfil three cumulative conditions:

- the pursuit of a legitimate interest by the controller or by a third party;
- the necessity to process personal data for the purposes of pursuing the legitimate interest;
- the interests or fundamental freedoms and rights of individuals do not take precedence over the legitimate interest(s) of the controller or of a third party (balancing exercise).

First of all, only the interests that are lawful, clearly and precisely articulated, real and present may be considered legitimate. For example, such legitimate interests could exist in a situation where the individual is a client or in the service of the controller.

Second, if there are reasonable, just as effective, but less intrusive alternatives for achieving the interests pursued, the processing may not be considered to be necessary. The necessity of a processing should also be examined with the principle of data minimisation.

Third, the controller must ensure that its legitimate interest is not overridden by the individual's interests, fundamental rights or freedoms. In this balancing exercise, the controller needs to take into account the interests of the individuals, the impact of the processing and their reasonable expectations, as well as the existence of additional safeguards which could limit the impact on the individual.

In addition, these Guidelines explain how this assessment should be carried out in practice, including in a number of specific contexts such as fraud prevention, direct marketing and information security. The document also explains the relationship between this legal basis and a number of data subject rights under the GDPR.

The Guidelines will be subject to public consultation until 20 November 2024.

---

9 October 2024 - European Data Protection Board: Opinion on Article 28 of the GDPR and on certain obligations arising from the designation of the External Data Processor (and sub-processors) adopted.

Art. 64(2) GDPR provides that any DPA can ask the Board to issue an opinion on matters of general application or producing effects in more than one Member State. Following an Art. 64(2) GDPR request to the Board by the Danish Data Protection Authority (DPA), the EDPB enacted an Opinion about situations where controllers rely on one or more processors and sub-processors.

In particular, the Opinion addresses eight questions on the interpretation of certain duties of controllers relying on processors and sub-processors, as well as the wording of controller-processor contracts, arising in particular from Art. 28 GDPR.

The Opinion explains that controllers should have the information on the identity (i.e. name, address, contact person) of all processors, sub-processors etc. readily available at all times so that they can best

fulfil their obligations under Art. 28 GDPR. Besides, the controller's obligation to verify whether the (sub-)processors present 'sufficient guarantees' should apply regardless of the risk to the rights and freedoms of data subjects, although the extent of such verification may vary, notably on the basis of the risks associated with the processing.

The Opinion also states that while the initial processor should ensure that it proposes sub-processors with sufficient guarantees, the ultimate decision and responsibility on engaging a specific sub-processor remains with the controller.
The EDPB considers that under the GDPR the controller does not have a duty to systematically ask for the sub-processing contracts to check if data protection obligations have been passed down the processing chain. The controller should assess whether requesting a copy of such contracts or reviewing them is necessary for it to be able to demonstrate compliance with the GDPR.

In addition, where transfers of personal data outside of the European Economic Area take place between two (sub-)processors, the processor as data exporter should prepare the relevant documentation, such as relating to the ground of transfer used, the transfer impact assessment and the possible supplementary measures. However, as the controller is still subject to the duties stemming from Art. 28(1) GDPR on 'sufficient guarantees', besides the ones under Art. 44 to ensure that the level of protection is not undermined by transfers of personal data, it should assess this documentation and be able to show it to the competent Data Protection Authority.

---

9 October 2024 – European Data Protection Board: the right to erasure ('right to be forgotten') shall be the topic for the fourth Coordinated Enforcement Action (CEF).

The European Data Protection Board (EDPB) selected the topic for its fourth Coordinated Enforcement Action (CEF), which will concern the implementation of the right to erasure ('right to be forgotten') by controllers. Data Protection Authorities (DPAs) will join this action on a voluntary basis in the coming weeks and the action itself will be launched during the first semester of 2025.

The right to erasure (Art.17 GDPR) is one of the most frequently exercised data protection rights and one about which DPAs frequently receive complaints. The aim of this coordinated action will be, among other objectives, to evaluate the implementation of this right in practice. For example, this will be done by analysing and comparing the processes put in place by different controllers to identify the most important issues in complying with this right, but also to get an overview of best practices.

In a coordinated enforcement action, the EDPB prioritises a specific topic for DPAs to work on at national level. In the past three years, DPAs have already coordinated their national actions on different topics, namely: the use of cloud in the public sector, the designation and position of Data Protection Officers and the implementation of the right of access by data controllers.

The results of these national actions are then aggregated and analysed together to generate deeper insight into the topic and allowing for targeted follow-up on both national and EU level.

In 2023, the EDPB published the report on its first coordinated action on the use of cloud-based services by the public sector.

Earlier this year, the EDPB also published the report on the outcome of the second coordinated action on the designation and position of Data Protection Officers.

The report on the outcome of the 2024 coordinated action on the right of access will be adopted at the beginning of 2025.

Coordinated actions follow the EDPB's decision to set up a Coordinated Enforcement Framework (CEF) in October 2020. The CEF is a key action of the EDPB under its 2024-2027 Strategy, together with the Support Pool of Experts (SPE). The two initiatives aim to streamline enforcement and cooperation among DPAs.

4 October 2024 – EU Court of Justice: an online social network such as Facebook cannot use all of the personal data obtained for the purposes of targeted advertising, without restriction as to time and without distinction as to type of data.

The fact that Mr Maximilian Schrems has made a statement about his sexual orientation on the occasion of a public panel discussion does not authorise the operator of an online social network platform to process other data relating to his sexual orientation, obtained, as the case may be, outside that platform, with a view to aggregating and analysing those data, in order to offer him personalised advertising.

Maximilian Schrems brought an action before the Austrian courts challenging the, in his submission unlawful, processing of his personal data by Meta Platforms Ireland in the context of the online social network Facebook. Those data include inter alia data concerning his sexual orientation. Meta Platforms Ireland collects the personal data of Facebook users, including Maximilian Schrems, concerning those users' activities both on and outside that social network, including in particular data relating to online platform visits and third-party websites and apps. To that end, Meta Platforms Ireland uses 'cookies', 'social plug-ins' and 'pixels', embedded on the relevant websites. With the data available to it, Meta Platforms Ireland is also able to identify Maximilian Schrems' interest in sensitive topics, such as sexual orientation, which enables it to direct targeted advertising at him in that regard, the question then arises as to whether Maximilian Schrems manifestly made public sensitive personal data about himself by having disclosed, on the occasion of a public panel discussion, the fact that he was homosexual, and thus authorised the processing of those data under the General Data Protection Regulation (GDPR).

In that context, the Supreme Court, Austria, requested the Court of Justice to interpret the GDPR.

First, the Court replies that the principle of data minimisation provided for by the GDPR precludes all of the personal data obtained by a controller, such as the operator of an online social network platform, from the data subject or third parties and collected either on or outside that platform, from being aggregated, analysed and processed for the purposes of targeted advertising without restriction as to time and without distinction as to type of data.

Second, the Court finds that the possibility cannot be ruled out that, by his statement on the occasion of the panel discussion in question, Maximilian Schrems manifestly made his sexual orientation public. It is for the Supreme Court, Austria, to verify whether this is so.

The consequence of the fact that a data subject has manifestly made public data concerning his or her sexual orientation is that those data may be processed in compliance with the provisions of the GDPR. However, that fact alone does not authorise the processing of other personal data relating to that data subject's sexual orientation.

Thus, the fact that a person has made a statement about his or her sexual orientation on the occasion of a public panel discussion does not authorise the operator of an online social network platform to process other data relating to that person's sexual orientation, obtained, as the case may be, outside that platform using partner third-party websites and apps, with a view to aggregating and analysing those data, in order to offer that person personalised advertising.

---

4 October 2024 – EU Court of Justice: Member States may make provision for competitors of the person allegedly responsible for an infringement of the laws protecting personal data to challenge that infringement in court as a prohibited unfair commercial practice.

The German Federal Court of Justice is to resolve a dispute between two German pharmacists. The pharmacist who owns the 'Lindenapotheke' pharmacy has been marketing pharmacy-only medicinal products on Amazon since 2017. Customers must enter certain information when ordering these medicinal products online.

On the basis of the German legislation on unfair commercial practices, a competing pharmacist applied to the German courts for an order that the owner of Lindenapotheke cease that activity so long as there is no guarantee that customers will be able to give their prior consent to the processing of data concerning health. The courts at first and second instance held that that marketing activity amounted in fact to an unfair and unlawful practice, since it is contrary to the Regulation on the protection of personal data (GDPR). In the absence of explicit consent from the customers purchasing those medicinal products, the sale entails processing of data concerning health that is prohibited under that regulation.

The German Federal Court of Justice wonders whether the national legislation, which allows a competitor to bring legal proceedings against the person allegedly responsible for infringements of the GDPR on the basis of the prohibition of unfair commercial practices, is consistent with that regulation. Indeed, according to the GDPR, it is in principle for the national supervisory authorities to monitor and enforce that regulation and for the data subjects (in this case, the customers) to defend their rights.

The German court also wishes to know whether the information entered when pharmacy-only medicinal products are purchased online constitutes data concerning health within the meaning of the GDPR, even where those medicinal products do not require a prescription. It therefore turned to the Court of Justice.

The Court replies, in the first place, that the GDPR does not preclude national legislation which, alongside the rights and powers conferred by the GDPR on the national supervisory authorities, on data subjects and on associations representing those persons, allows competitors of the person allegedly responsible for an infringement of the laws protecting personal data to bring legal proceedings against that person, for infringements of that regulation, on the basis of the prohibition of unfair commercial practices. On the contrary, this undoubtedly contributes to strengthening the rights of data subjects and ensuring that they enjoy a high level of protection. Moreover, this may be particularly effective, in so far as a large number of GDPR infringements could thus be prevented.

In the second place, the Court finds that information entered by customers (such as their name, the delivery address and the information required for individualising the medicinal products) when ordering pharmacy-only medicinal products online constitutes data concerning health within the meaning of the GDPR, even where the sale of those medicinal products does not require a prescription. Those data are capable of revealing information about the health status of an identified or identifiable data subject by means of an intellectual operation involving comparison or deduction because a link is established between that person and a medicinal product, its therapeutic indications or its uses, irrespective of whether that information concerns the customer or any other person for whom the customer places the order.

Accordingly, in the absence of a prescription, it is immaterial whether it is only with a certain degree of probability and not with absolute certainty that those medicinal products are intended for the customers who ordered them. To make a distinction according to the type of medicinal product and to whether or not the sale of those medicinal products requires a prescription would be contrary to the GDPR's objective of ensuring a high level of protection. Consequently, the seller must inform those customers in an accurate, comprehensive and easily understandable manner of the specific characteristics and purposes of the processing of those data and request their explicit consent to that processing.

---

4 October 2024 - EU Court of Justice: the limits of legitimate interest as a basis for the lawfulness of processing for marketing and commercial purposes.

An association of Dutch tennis clubs communicated the data of its members, without their consent, to external third parties (certain sponsors), including a company marketing sports products, and to 'Nederlandse Loterij Organisatie BV', the largest gambling and casino games company in the Netherlands. The latter paid the association a fee for making available the personal data of its members (names, addresses, dates of birth, landline and mobile telephone numbers, e-mails). This data was then used for a campaign of promotional calls by the call centres used by the gaming company.

Following the sanction imposed by the Dutch Garante on the sports association, the latter challenged the measure, arguing that the processing was lawful on the basis of legitimate interest under Article 6(1)(f) of the GDPR.

The judges therefore turned to the Court of Justice asking how the expression 'legitimate interest' in point (f) of the first paragraph of Article 6(1) of the GDPR should be interpreted, and in particular whether 'legitimate interest' should be understood to mean exclusively an interest that is enshrined and determined by a law, which is considered deserving of protection by the Union legislator or the national legislator or whether the legitimate interest need not necessarily derive from a fundamental right or a legal principle, but any interest may constitute a legitimate interest unless it is contrary to law, and that interest must therefore be assessed according to a 'negative criterion'.

The Dutch courts ask in particular whether a strictly commercial interest and interest such as the one at issue, namely the provision of personal data in return for payment without the data subject's consent, may in certain circumstances be regarded as a legitimate interest. If so, what circumstances determine whether a strictly commercial interest is a legitimate interest.

The EU Court has clarified that a processing of personal data consisting in the communication of personal data of members of a sports federation against payment in order to satisfy a commercial interest of the data controller (that is to say, the association transmitting the data) may be regarded as necessary for the purposes of the legitimate interest pursued by that controller only on condition that that processing is strictly necessary for the purposes of the legitimate interest in question and that, in the light of all the relevant circumstances, the interests or the fundamental freedoms and rights of those members do not override that legitimate interest. Although that provision does not require that such an interest be determined by law, it does require that the legitimate interest invoked be lawful. Moreover, if it is possible to ask data subjects for their consent to the processing and communication of their data for marketing purposes, then legitimate interest is not a basis for the lawfulness of processing that can be properly invoked and used in such cases.

Finally, the judgment emphasises that legitimate interest cannot be a basis for the processing of data of data subjects if there is communication to a gambling company, given the risk of exposing those persons (then recipients of commercial calls) to the danger of developing gambling diseases.

---

4 October 2024 - EU Court of Justice: conditions for exercising the right to delete personal data from the Business Register held by a Member State and for claiming compensation for non-material damage in the event of a refusal.

The Court of Justice of the European Union (CJEU) published its judgment in Case C-200/23, concerning the Agentsia po vpisvaniyata's (the Registry Entries Agency of Bulgaria) refusal to delete certain personal data concerning an individual contained in a partnership agreement published in the commercial register under the General Data Protection Regulation (GDPR).

The CJEU outlined that the individual was a partner of a limited liability company under Bulgarian law. On July 8, 2021, the individual asked the Agency to delete the personal data concerning them contained in the said partnership agreement, specifying that they wanted to withdraw consent. In the absence of a response from the Agency, the individual brought the matter before the Administrative Court of Dobrich which annulled the Agency's implied refusal to delete the data and referred the case back to the Agency for a new decision. The Agency indicated, by a letter, a certified copy of the relevant partnership agreement concealing the individual's personal data, with the exception of that required by law. The individual again brought an action before the Administrative Court seeking the annulment of the letter and an order against the Agency to compensate it for the non-pecuniary damage of the letter, which infringed the rights conferred by the GDPR. The Administrative Court annulled the letter and ordered the Agency to compensate the individual for non-pecuniary damage, pursuant to Article 82 of the GDPR. The Agency appealed to the Supreme Administrative Court which subsequently referred the case to the CJEU.

The CJEU found, among other things, that Directive 2017/1132 must be interpreted as meaning that it does not impose on a Member State an obligation to authorize the publication, in the commercial register, of a partnership contract subject to the mandatory publication provided for by the Directive and containing personal data other than the minimum personal data required, the publication of which is not required by the law of that Member State.

Additionally, the CJEU found that Articles 4(7) and 4(9) of the GDPR must be interpreted as meaning that the authority keeping the commercial register of a Member State which publishes, in that register, the personal data contained in a partnership contract subject to the mandatory publication provided for by the Directive, which was sent to it in the context of an application for registration by the company, is both the recipient of the data and, in particular in so far as it makes them available to the public, the controller of that data, even where that contract contains personal data not required by the Directive or by the law of that Member State.

Moreover, the CJEU held that Article 82(1) of the GDPR must be interpreted as meaning a loss of control for a limited period by the data subject over their personal data due to the making available to the public of such data online in the commercial register of a Member State which may be sufficient to cause 'non-material damage,' provided that that person demonstrates that they actually suffered such damage, however minimal, without that concept of 'non-material damage' requiring the demonstration of the existence of additional tangible negative consequences.

---

4 October 2024 - CJEU publishes judgment on compensation for non-pecuniary damages under the GDPR.

The Court of Justice of the European Union (CJEU) published its judgment in Case C-507/23 regarding compensation for non-pecuniary damages under the General Data Protection Regulation (GDPR).

The CJEU outlined that the applicant is a journalist who is an expert in the automotive field. The applicant requested the Consumer Rights Protection Center of Latvia (PTAC) to remove a video campaign that featured a character imitating the applicant without their consent and compensation for reputational damage. The applicant brought an action before the District Administrative Court of Latvia which ordered PTAC to stop the video campaign and to pay compensation. On appeal to the Regional Administrative Court of Latvia, PTAC's actions were declared unlawful but the request for damages was dismissed as it held that the intention of the video campaign was to carry out a task in the public interest, not to harm the reputation of the applicant.

The Supreme Court of Latvia asked the CJEU to issue a preliminary ruling to clarify whether:

- article 82(1) of the GDPR is to be interpreted as meaning that unlawful processing may in itself constitute an unjustified interference with the right to data protection and cause harm to that person;
- article 82(1) of the GDPR allows for the order of an apology as a sole remedy for non-pecuniary damages; and
- article 82(1) of the GDPR allows for circumstances revealing the intention and motivation of the controller to justify lesser compensation for the damage.

The CJEU found that:

- a breach of the GDPR is not sufficient in itself to constitute 'damage' within the meaning of Article 82(1) of the GDPR, read in light of Article 8(1) of the Charter of Fundamental Rights;

- the presentation of an apology may constitute adequate compensation for non-pecuniary damage, in particular, where it is impossible to restore the situation to the state prior to the occurrence of that damage, provided that the form of compensation is capable of fully compensating for the harm suffered; and

- Article 82(1) of the GDPR precludes the attitude and motivation of the controller from being taken into account whether to grant the data subject lesser compensation.

ARTIFICIAL INTELLIGENCE.

14 October 2024 - EU Council: Directive on digital platform workers finally approved.

The process of approving new rules aimed at improving the working conditions of all those working in digital platforms in the EU comes to an end: the EU Council has adopted the directive on platform work, which will now be published in the EU Official Journal.

The new directive aims to promote greater transparency in the use of algorithms that manage human resources, ensuring that automated systems are monitored by qualified personnel and that decisions taken in this way can be challenged by workers.

The new directive also aims to correctly determine the employment status of persons working at digital platforms, giving them access to the rights that all workers should enjoy. To this end, Member States will establish a legal presumption of employment that will be activated when certain facts are found that are symptomatic of control and direction.

From the moment of publication in the EU Official Journal, Member States will have two years to transpose the provisions into national law.

---

11 October 2024 – G7 Data Protection Authorities: the role of DPAs in regulating Artificial Intelligence.

During the fourth meeting of the G7 Data Protection Authorities, coordinated this year by the Italian Data Protection Authority, the Authorities agreed on the importance of the role of the Authorities in the regulation of AI, determined precisely in order to ensure its reliability. In fact, it was emphasized that they have the skills, as well as the independence, necessary to ensure indispensable guarantees to govern such a complex phenomenon. It was therefore agreed on the opportunity to express to governments the desire for the recognition of an adequate role for data protection authorities in the overall AI governance system. The Data Protection Authorities also decided to monitor the legislative developments of AI and the role of the Privacy Authorities within the jurisdictions involved.

This, as well as other objectives, are contained in the Action Plan, the document that looks to the future of the G7 by establishing its intentions and thematic areas that will be the subject of next year's work. The comparison between the legal systems of the different countries on the issue of the free flow of data, which represents an important element of development and progress, including economic and social progress, has also proved to be very useful.

DIGITAL MARKETS

10 October 2024 - Legislative decree 144/2024 for the harmonisation of national legislation with the provisions of Regulation (EU) 2022/868 on European data governance published in the Official Gazette.

The Italian legislative decree identifies *AgiD – Italian Digital Agency* as the national authority, which will have regulatory and sanctioning responsibilities and functions. In fact, AgiD will be the competent body to assist public bodies from which data are requested, it will act as a one-stop shop to sort data requests to public bodies (first pillar of the DGA), it will play the role of competent authority for data brokerage services (data sharing, second pillar of the DGA) and it will deal with the registration of organisations for data altruism (third pillar of the DGA). It will be able to impose sanctions ranging from EUR 10 to 100,000 or up to 6% of the previous year's global turnover in the event of a breach of the ADI rules.

The legislative decree is of fundamental importance because it finally renders operational a regulatory framework (in any case applicable from 24 September 2023) that unleashes the potential and business opportunities of the so-called European Data Strategy, opening up for businesses - for example - opportunities for further development of goods and services through access to and sharing of the relevant information assets held by public administrations (the first pillar of the ADI: re-use of data held by public entities) or through the development of new data inter-mediation services (second pillar of the DGA) in which the enterprise brings together for the conclusion of a commercial licence to use data (personal and non-personal) those who have the right to access the data (the so-called 'data owner') and those who want to use that data (the so-called 'data user').

---

10 October 2024 - EU Council: Cyber Resilience Act (CRA) definitively approved, introducing new security requirements for digital products.

The EU Council has finally approved the Cyber Resilience Act, the new law that introduces cyber security requirements for products with digital elements to ensure that, for example, connected home cameras, refrigerators, TVs and toys are secure before they are placed on the market. The overall aim is to close gaps, clarify linkages and make the existing cybersecurity legislative framework more coherent, ensuring that products with digital components are secure along the supply chain and during their life cycle.

The regulation will apply to all products that are directly or indirectly connected to another device or network. There are some exceptions for products for which cyber security requirements are already laid down in existing EU standards, e.g. medical devices, aeronautical products and cars.

Specifically, the text provides for the introduction of EU-wide cybersecurity requirements for the design, development, production and making available on the market of hardware and software products, in order to avoid overlapping requirements stemming from different member state regulations. For example, software and hardware products will bear the CE marking to indicate that they comply with the requirements of the regulation.

It will also enable consumers to take cybersecurity into account when selecting and using products containing digital elements, making it easier for them to identify hardware and software products with the appropriate cybersecurity features.

The act will now be signed by the Presidents of the Council and the European Parliament and then published in the Official Journal of the EU.

---

9 October 2024 - European Banking Authority: Guidelines for issuers of asset reference tokens (ARTs) and electronic money tokens (EMTs) to ensure orderly and timely redemption of tokens in the event of an issuer's inability to fulfil its obligations.

The EBA's Final Report on Redemption Plans, pursuant to Articles 47 and 55 of Regulation (EU) 2023/1114, sets out guidelines for issuers of asset reference tokens (ARTs) and electronic money tokens (EMTs) to ensure an orderly and timely redemption of tokens in the event of an issuer's inability to fulfil its obligations.

The guidelines include strategies for liquidating reserve assets, token holder profiling, anti-money laundering procedures and liquidity risk management. The redemption plan must ensure the fair treatment of all token holders, with the aim of minimising economic damage and ensuring market stability.

INFORMATION TECHNOLOGY

8 October 2024 – Internal Revenue Agency: provision no. 379575/2024 on the procedures for communicating, changing and revoking data relating to the special digital domicile and for confirming or revoking the PEC address

With provision no. 379575 of 7 October 2024, the Inland Revenue provided clarifications on the procedures for electing a special digital domicile and for confirming or revoking digital addresses already communicated, pursuant to Article 60-ter, paragraph 5, of Presidential Decree no. 600/1973.

The procedure does not apply to companies and professionals whose PEC addresses must be registered in the National Index of digital domiciles of companies and professionals (INI-PEC). Only natural persons, professionals and other private law entities not required to be registered in professional registers, lists or registers or in the business register may elect a special digital domicile. Such persons may elect only one special digital domicile.

The special digital domicile is elected by means of the specific function available in the reserved area of the Internal Revenue Agency website. The date on which the service for communicating such domicile will be made available will be announced in a specific communication published on the website of the Revenue Agency.

The Agency will send a message containing a validation code to the special digital domicile indicated in order to verify its existence and actual availability to the applicant. The entry of the validation code within the user's reserved area successfully concludes the verification and takes effect for the purposes of notifications and communications.

Changes to the special registered digital domicile are communicated in the same way; revocation is communicated by means of a special function.

---

2 October 2024 – Legislative Decree No. 138/2024, transposing Directive (EU) 2022/2555 NIS 2 on a common level of cybersecurity in the EU, will enter into force on 16 October.

Legislative Decree No. 138 of 4 September 2024 on the 'Transposition of Directive (EU) 2022/2555 on measures for a high common level of cybersecurity in the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148' was published in Official Gazette No. 230/2024.

Legislative Decree No. 138/2024, which will enter into force on 16 October 2024, establishes measures to ensure a high level of cybersecurity in the national sphere, contributing to increasing the common level of security in the EU so as to improve the functioning of the internal market.

The Decree, consisting of 44 articles, specifically provides for:

(a) the National Cybersecurity Strategy, containing forecasts aimed at ensuring a high level of cybersecurity;

b) the integration of the cyber crisis management framework, in the context of the national organisation for the management of crises involving aspects of cybersecurity;

(c) the confirmation of the National Cybersecurity Agency as:

1) National NIS Competent Authority, regulating its powers inherent to the implementation and enforcement of the Decree;

2) NIS Single Point of Contact, ensuring national and cross-border liaison;

3) National Information Security Incident Response Team (CSIRT Italy);

d) the designation of the National Cybersecurity Agency, acting as coordinator pursuant to Article 9(2) of Directive (EU) 2022/2555, and the Ministry of Defence, each for the areas of competence indicated in Article 2, c. 1(g), as National Large-Scale Cyber Crisis Management Authorities, ensuring consistency with the existing national framework for general cyber crisis management, without prejudice to the tasks of the Cyber Security Unit referred to in Article 9 of Decree-Law No. 82/2021;

e) the identification of NIS Sector Authorities that cooperate with the National Cybersecurity Agency, supporting its functions as NIS Competent National Authority and NIS Single Point of Contact;

f) the indication of the criteria for the identification of the entities to which this Decree applies and the definition of the relevant obligations with regard to cybersecurity risk management measures and incident reporting;

(g) the adoption of cooperation and information sharing measures for the purposes of applying the decree, in particular, through national participation in

1) to the NIS Cooperation Group between NIS competent authorities and between single points of contact of EU Member States, with a view to increasing trust and cooperation at EU level;

(2) to the Cyber Crisis Liaison Organisations Network (EU-CyCLONe) in order to support the coordinated management of large-scale cyber incidents and crises at operational level and to ensure the regular exchange of relevant information between Member States and EU institutions, bodies, offices and agencies

(3) the network of national CSIRTs with a view to ensuring rapid and effective technical cooperation.

INTELLECTUAL PROPERTY

10 October 2024 - The IP measures in the Omnibus Decree, converted into Law 143/2024.

Article 6-bis of Decree-Law No. 113/2024, amended Law No. 93 of 2023. With the amendments - and premised that under Article 2, the Communications Guarantee Authority (AGCM) may order service providers, including network access providers, to disable access to abusively disseminated content by blocking the resolution of the Data Source Name (DNS) of domain names and blocking the routing of network traffic to IP addresses uniquely intended for unlawful activities - now IP number assignment service providers shall periodically re-enable the resolution of domain names and the routing of network traffic to blocked IP addresses, at least six months after blocking, if they are not used for unlawful purposes. In addition, AGCOM, in order to ensure the effective execution of inhibition orders, sets, limited to the first year, maximum quantitative limits of IPs that can be blocked at the same time.

The Omnibus Decree also introduced for anti-piracy purposes a new Article 174-*bis* to the Copyright Law 633/1941. The new provision imposes specific reporting and communication obligations - the violation of which is punishable by imprisonment of up to one year and fines for computer crimes and unlawful processing of data under Article 24-bis of Legislative Decree No. 231 of 8 June 2001 on business offences. 231 on business offences - for providers of network access services, search engine operators and information society service providers, including providers and intermediaries of VPNs or in any case of technical solutions that obstruct the identification of the source IP address, content delivery network operators, providers of internet security services and distributed DNS, who place themselves between visitors to a site, and hosting providers who act as reverse proxy servers for websites.

These entities must also designate and notify AGCOM of a contact point enabling them to communicate directly, electronically, with the Authority. In addition, those who are not established in the EU but who offer services in Italy must designate in writing a natural or legal person to act as their legal representative in Italy to enable them to communicate directly, electronically, with the Authority.