CHIOMENTI

Newsletter

IP, TMT and Data Protection Department
February 2021

SUMMARY

I EDPB GUIDELINES ON EXAMPLES REGARDING DATA BREACH NOTIFICATION

On 14 January 2021, the European Data Protection Board ("**EDPB**") adopted and publicly consulted the Guidelines 01/2021 on examples regarding data breach notification. These Guidelines are intended to complement the Guidelines WP 250 (adopted in 2018) and reflect the common experiences of national supervisory authorities ("**DPAs**") - since the entry into application of the General Data Protection Regulation ("**GDPR**") - by introducing more practice-oriented, case-based guidance and recommendations.

The GDPR (Art. 4(12)) defines a "personal data breach" as 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*».

The purpose of the Guidelines is to help data controllers in deciding how to handle data breaches and what factors to consider during risk assessment. Under this perspective, the Guidelines would result consistent with the tools – such as self-assessment mechanisms to identify actions to be taken in case of personal data breach – made available by the Italian Data Protection Authority with a view to supporting data controllers in relation to events of breach (here is the *link* to the section of the Italian Data Protection Authority's website dedicated to personal data breaches).

The Guidelines contain a wide array of case studies – which are based on typical cases from the DPAs' collective experience with data breach notifications – structured according to different categories of data breach, such as ransomware attack, data exfiltration, and lost or stolen devices and paper documents. Based on a case category, the Guidelines shed light on the most typical good or bad practices, advice on how risks should be

identified and assessed, highlight the factors that should be given consideration, as well as inform in which cases the controller should notify the DPA and/or notify the data subjects.

Moreover, the Guidelines remind that, pursuant to the GDPR, the internal documentation recording the breach - which is prepared by the controller - is an obligation independent of the risks pertaining to the breach, thus it must be performed regardless of the specific case relevant to the controller.

The end date for providing feedbacks in the context of the public consultation is 2 March 2021.

Here is the *link* where you can view the text of the Guidelines.

II ITALIAN DATA PROTECTION AUTHORITY GUIDELINES ON COOKIES AND OTHER TRACKING SYSTEMS

On November 26, 2020, the Italian Data Protection Authority (hereinafter, "**IDPA**") adopted and publicly consulted new Guidelines for the use of cookies by web site managers. The consultation ended on 10 January 2021.

The IDPA decided to address again the issue of the use of cookies and other tracking systems in order to complement its previous analysis on the subject in 2014 and 2015, following the indications provided by the European Data Protection Board (EDPB) in the Guidelines of 4 May 2020 (Guidelines 05/2020 on consent under Regulation 2016/679).

Among the main innovations we mention the need to abandon certain practices for the collection of consent, such as the 'scrolling down' of a web page to give consent to the installation of cookies on the user's device. In this regard, the Authority has defined the scrolling unsuitable for the collection of an unequivocal consent, «*except in the sole event that it is included in a more structured process in which the user is able to generate an event, recordable and documentable at the server of the site, which can be qualified as a positive action suitable to unequivocally manifest the will to give consent to treatment*».

Another important clarification concerns the use of the so-called 'cookie wall', namely the 'take it or leave it' mechanism in which the user is asked to express his consent to the reception of profiling cookies, otherwise it will not be able to access the site. For the IDPA, this mechanism would be unlawful under the GDPR except in the event that the user is offered the opportunity to access an equivalent content or service without giving consent to the installation and use of cookies.

Moreover, the Authority reviews the category of analytics cookies by circumscribing them within the scope of the new principles of data protection by design and by default. In this regard, it should be noted that before the entry into force of the GDPR, analytical cookies were included among the technical cookies and, as such, could be used without the prior acquisition of consent by the user. In light of the current applicable legal framework, the IDPA has found it necessary to restrict the power of identification of analytical cookies, including third-party ones, comparing them, in terms of exemption from the acquisition of consent, to technical cookies only if: (i) they are used only to produce aggregate statistics and in relation to a single site or a single mobile application; (ii) at least the fourth component of the IP address is masked; (iii) the third parties refrain from combining such cookies with other processing (customer files or statistics of visits to other sites, for example) or from transmitting them to third parties.

With regard to the privacy policy uploaded on the site, according to the IDPA this should contain a simple and accessible language and be made in multilayer and multichannel mode. If only technical cookies are used, the relative information can be placed in the home page of the site or in the general information. On the contrary, if other cookies are also used, the Authority recommends the use of banners with an immediate pop-up and of adequate size containing a series of information such as, for example, the indication that the site uses technical cookies and, subject to the user's consent, profiling cookies; the link to the privacy policy containing the complete information; the link to another area where it is possible to choose in an analytical way the functionalities, the third parties and the cookies to be installed; and a command to close the banner without giving consent to the use of cookies or other profiling techniques maintaining the default settings.

Also, in relation to the usability of the website, the Authority also stresses that it is not necessary to reiterate the request for user's consent, except if one or more of the conditions under which it was collected change or when it is impossible for the site to know whether a cookie has already been stored in the device.

Finally, the Guidelines refer to additional tracking systems other than cookies. Among these there are other 'passive' identification tools, such as the so-called fingerprinting that allows to identify the device used by the user through the collection of information relating to the specific configuration of the device itself adopted by the data subject. On this point, it should be noted that, unlike 'active' systems (such as cookies) for which the user who does not want to be profiled also has the practical possibility of removing them directly, since they are stored in his or her device, with fingerprinting the user does not have autonomously operable tools and must necessarily resort to the action of the data controller.

Here is the *link* where you can view the text of the Guidelines.

III RIGHT TO COMPENSATION FOR NON-PECUNIARY DAMAGE AND UNLAWFUL CIRCULATION OF PERSONAL DATA

The Italian Supreme Court (*Corte Suprema di Cassazione*), with judgment no. 29982/2020 filed on 31 December 2020, declared inadmissible and ungrounded the appeal filed by a school employee against judgment no. 2150/2015 of the Court of Turin, which had in turn rejected the request for compensation for the damage suffered by the plaintiff due to the unlawful disclosure of certain information about him.

The plaintiff had turned to the Turin Court complaining that the director of the school where the employee is employed had disclosed to the police news about disciplinary charges against the employee and that, following this disclosure, the news had circulated within the school, thus causing the plaintiff humiliation, discomfort and embarrassment.

These complaints had been rejected by the Court of Turin for the following four concurrent and self-standing reasons: (i) the necessity of the communication of personal data for institutional purposes; (ii) the extraneousness of the conduct of the director to the circulation of the news in the staff of the school; (iii) the lack of proof of the damages-consequences suffered; (iv) the lack of a minimum standard of seriousness to give rise to a non-pecuniary damage compensation.

In light of the above, the employee appealed to the Italian Supreme Court, without, however, objecting to the reason referred to in point (ii) above.

In rejecting the grounds for appeal put forward by the employee, the Supreme Court made it clear, *inter alia*, that the failure to challenge or the groundlessness or inadmissibility of the grounds raised to one of the reasons renders also inadmissible, due to an intervening lack of interest, the grounds relating to the other reasons explicitly objected to, as the latter grounds could not in any event lead, given the intervening finality of the other reasons, to the review of the decision itself.

In addition, with reference to the third ground of appeal (failure to prove the damage-consequences suffered) the Court stated that, in the case in question, the prejudice and consequent damage did not meet the minimum standards of seriousness required by law to overcome the threshold of tolerance imposed by the constitutional duty of solidarity, as the information circulated concerned simple objections made to the employee (and not real disciplinary measures), without specific references.

In this regard, the Court referred to recent case law in reiterating how the non-pecuniary damage compensable under the - now repealed - Article 15 of Legislative Decree No. 196/2003 (Italian Privacy Code) needs to meet the standards of the "seriousness of the prejudice" and the "seriousness of the damage", for this right the balance with the principle of solidarity under Article 2 of the Italian Constitution operates. Therefore, concludes the Court, to determine an unjustifiable prejudice of the right is not the mere violation of the requirements laid down by the Italian Privacy Code, but only the violation that significantly offends its actual scope, being, however, the assessment of the fact remitted to the judge.

IV RIGHT TO BE FORGOTTEN, NO REMOVAL OF AN ARTICLE WRITTEN BY A DECEASED PERSON WITHOUT A SUBSTANTIAL INTEREST

With decision issued on 29 October 2020 [web doc no. 9509538], the IDPA reiterated that there must be a substantial interest to be protected in order to remove from a website an article written by a person, now deceased.

The son of the deceased author had, in his capacity as heir, sent the request for removal of the article both to the manager of the website where the article had been published and to Google. While the search engine had taken steps to de-index the URL referable to the disputed content, the web manager opposed the son's request. Against this opposition, the applicant lodged a complaint with the IDPA requesting the cancellation of the article, claiming that its content was detrimental to the reputation of himself and his family. In support of the complaint the son declared to act also in the interest of the deceased father, claiming that the latter had allegedly written the article at a time when he was already undermined by an illness that would have reduced his mental capacity.

In this respect, it should be reminded that Art. 2-*terdecies* of Legislative Decree n. 196 of 30 June 2003 (s.c. Privacy Code) provides for the possibility of lodging a complaint regarding the exercise of rights belonging to a deceased person in order to assert an interest of the complainant or of the *de cuius* himself or for family reasons worthy of protection.

In light of with the complaint, the IDPA found that, up to the time of his death, the deceased had never requested the removal of the published content, nor had he otherwise manifested the will to disown its content, a will of which no evidence was presented by the claimant son. Therefore, the Authority stated, the existence of an interest on the part of the *de cuius* in the cancellation of the article could not be considered proven; on the contrary, the article retains its own historical value as a testimony of the life of a deceased person and free expression of the latter's freedom of expression.

However, the IDPA, as several years have passed since the publication of the article (16 years) and the death of the author (6 years), has ordered the manager of the website not to make the writing available through external search engines, in order to balance the need to preserve the writing with the interest of the family members mentioned therein.

Here is the *link* to where you can view the text of the decision.

Contacts

Gilberto Nava
Partner – Chiomenti
IP, TMT, Data Protection
T. +39.06.46622.719
gilberto.nava@chiomenti.net

Giulio Vecchi
Counsel – Chiomenti
IP, TMT, Data Protection
T. +39.0272157658
giulio.vecchi@chiomenti.net