

# The collecting of consent to the processing of children's personal data, between volatility and disobedience

Juanita Goicovici<sup>1\*</sup>

<sup>1</sup> Babeş-Bolyai University of Cluj-Napoca, Romania

**Abstract.** The paper addresses the problematics of collecting consent to the processing of children's personal data, observing the connection between granularity and the specificity of consent and insisting on the triple level of granularity which may be seen as applicable: (i) the granularity of the first degree, relative to the delimitation by reference to the consent granted at the formation of the main contract; (ii) secondary degree of granularity, relating to the sequencing of processing purposes; (iii) tertiary granularity, regarding the taxonomic specificity of the processing operations; in the case of children's consent, this specific protection is expected to apply particularly to the use of children's personal data for marketing or profiling purposes and to the collection of personal data when using services directly offered to children, whose capacity to exercise rights in this matter can be established in national law as beginning at the age of 16, without being able to go below the 13-year threshold, as provided by Article 8, para. (1), second thesis of General Regulation 2016/679. Related to the purposes of the processing, the data operator must inform the child, in an unambiguous and structured way, of the purposes of the processing of personal data, so that the latter were able to express the consent for each of the purposes, in a differentiated manner without being forced to accept them in their entirety, a requirement that functions as a safeguard against the gradual expansion or blurring of the clarity of the processing purposes. In relation to the holder of responsibility or parental authority, Regulation (EU) 2016/679 imposes on the data controller an obligation of diligence, in order to verify whether the holder of responsibility or parental authority has granted or authorized the granting of consent, taking into account the available technologies (as selected by the parent), which is a requirement that implies, for data controllers, the fact that they are expected to check not only the existence of consent (when processing the child's personal data), but also the provenience of this consent.

---

\* Corresponding author: [juanita.goicovici@law.ubbcluj.ro](mailto:juanita.goicovici@law.ubbcluj.ro)

## 1 Introductory Remarks

Children's vulnerability, in terms of personal data collecting and processing, represents a saliently problematic legal territory, constantly alimeted by the increasingly augmented appetite for social media exposure, the risk-plethora of which is often ignored, either by the child or by the legal representatives of the latter (parents and tutors). This study approaches the issue of the requirement of granular consent, legitimating the processing of children's personal data and as the basis of the legitimacy of the data collecting and data processing operations in which the data controllers are engaged. The central point of this twofold approach is represented in Article 5, 1<sup>st</sup> para., let. (b) of Regulation (EU) 2016/679, which imposes additional requirements on the manner of collecting personal data, specifying that these data can be collected for specific, explicit, and legitimate purposes, without being subject to processing operations which are incompatible with these primary goals. Highly provocative, the subject of collecting the consent to the processing of children's personal data continues to generate legal controversy, especially in terms of transparency of consenting. As pointed out by recent specialised scholarly analyses [1], in the perimeter of the obligations incumbent on professionals / data controllers to transparently inform data subjects, three cardinal rules can be distinguished: (I) the respecting of the exigencies derived from principle of informational amplitude, which requires that the information provided to the data subjects is expected to be complete, without omitting essential information; (ii) the principle of intelligibility of information, which refers to resorting to a comprehensible form of providing informative details; (iii) the principle of loyalty, from which the condition of correctness of the provided information follows, as an element of contractual loyalty [2], [3]. This 'tripod' on which the obligation to inform the data subjects is placed remains in the centre of the discussions on the legitimacy of the children's data collecting and processing, as an essential pillar which can be found, with prominent outlines also in the matter of data collecting and processing [4], [5]. On the other versant of the discussions, the inferior capacity of younger children in terms of deciding on their personal data exposure generated privacy concerns, which have led the European legislator to establish a limited timeframe of a minimum of 13 years-old for the child's expressing consent to personal data processing [2], [5].

Underpinning sequential issues on the manners under which children's data collection and processing is managed in the perimeter of children accessing health services, for example, or educational services, the interrogations on the legitimacy of data processing remain complex, due to the envisaged fact that, in a plethora of cases, it can be acknowledged that the data subjects under both categories (children and parents or legal guardians) are underestimating the implications of the manner in which their data are being captured and used, nor are the latter completely conscient of the prerequisites of risks associated to children's data processing or data transfer [6].

European data protection regulation reflects a pointillistic approach to regulation of children's data collecting and processing, while allowing the national legislator to establish time limits for the validity of child's consent expressed without the assistance of the adult guardian, yet not permitting the national frame of each member-state to lower the protection standards under the limit of 13-years old children, whose consent must be replaced by the adult guardian's agreement to the personal data collecting and processing [3], [7]. Nevertheless, the optimal legal protection of children's data gained attention particularly catalysed for hypotheses in which these sets of data were altered or ported to subsequent data controllers, in a context in which these conceptual themes are continuously provocative for legal practitioners [8], [9], [15].

Accommodating the solutions on the adequacy of the processing of children's personal data on the occasion of child-oriented services, the provisions of Regulation (EU) 2016/679 on the pertinency of the parental responsibility holder's consent (excepting the cases of

preventive or counselling services) are centred on the transparency exigencies resorting to easily readable language [2], [7]; particularly, in consent-based hypotheses of data processing, the adequate identification of the purposes set for data processing becomes of a more stringent nature in the perimeter of children's data collecting, even in cases in which it is the adult guardian or parent that is called to decide on the agreeing to child's data exposure [6], [10].

## **2 Specific requirements applicable to the collecting of consent for the processing of children's data**

### **2.1 Assertions on children over 16 years old's consent to the processing of personal data**

In the case of children's consent, the specific protection is expected to apply particularly to the use of children's personal data for marketing or profiling purposes and addressing the private information collected in hypotheses in which digital services were directed towards users under 16 years old. Their capacity to exercise rights in this matter can be established in national law as starting with the age of 16, without being allowed to lessen below the 13-year threshold, provided by Article 8, para. (1), second thesis of General Regulation 2016/679. Related to the issue of purpose selection, the data operator must inform the children, in an unambiguous and structured way [11], on the data collecting process, so that they would be able to express the consent for each of the purposes, in a differentiated manner without being forced to accept them in their entirety, a requirement that functions as a safeguard against the gradual expansion of initial purposes or altering the clarity of the processing purposes [17]. In relation to the holder of responsibility or parental authority, Regulation (EU) 2016/679 imposes on the data controller an obligation of diligence, in order to verify whether the holder of responsibility or parental authority has granted or authorized the granting of consent, taking into account the available technologies (as selected by the parent), which is a requirement that implies, for data controllers [13], the fact that they are expected to check not only the existence of consent (when processing the child's personal data) [14], but also the provenience of this consent [18], [19], [20]. The data controller's possibility to invoke the 'legitimate interest' excuse for the broader expansion of the use of children's data remains marginal and is expected to be used in a parsimonious manner. In such instances, the individual (child) user would have to learn the importance to change the account settings to 'private', otherwise permitting or facilitating third-parties access to personal information such as phone number and/or email address, thus considerably rendering the children vulnerable to malicious or malevolent actions [15], [16].

### **2.2 Parent's liability for the posting of excessive content, comprising the exposing of children's images on social media**

Currently, there is no specific national legislation intended to establish pertinent general rules in case parents post (excessive) content including children's images on social media, nor is the mentioned issue specifically addressed under European Union's regulations on data protection and privacy [22]. As resulting from the judicial practice at a national level [3], in cases of shared custody, the plaintiffs were requesting that the defendants be obliged to stop posting/distributing images, photos, videos, on social media platforms, at least not without the other parent's prior consent, until the age at which minors acquire the capacity to exercise their rights to privacy, a request which has been founded admissible in a court of law [3], on considerations pertaining to the other parent's right to oppose to the excessive exposure of

children's images by the parent having legal custody [3]. The main reasons for the applicant addressing the court were based on elements such as the fact that the parent sharing custody did not want children to be excessively exposed on social networks, since, in such situations, parents must give mutual permission to post photos of their children. Specifically, the judge may order the defendant (children's parent) to remove the photos of the children from parent's account on the social media platforms and forbade the defendant to post, show or otherwise distribute photos of the children on social networks, unless both parents reach a mutual agreement on the posting of each set of images.

As it has been emphasised in specialised literature [3], there is a salient distinction to be made between the hypotheses in which the dispute arose between the parents, and when the courts will be able to settle it by applying the rules regarding the content of the notion of 'parental authority' under national law, and, on the other versant of the discussion, the hypotheses when the dispute is established between the parent/parents and any other third party, even another family member (grandparents, collateral relatives etc.), the legal basis for solving the dispute concerning the use of children's data is found in the GDPR provisions [24], [25]. Doctrinal previous work established that, in the case of a dispute between parents, the dispute concerns the way of exercising the parental authority, namely the manner under which each parent decides in the interest of his/her own child. A dispute between the parents, on the one hand, and the third-party who processed the child's image, on the other hand, becomes a dispute regarding the processing of personal information [3].

The issue of clarifying the existence of the legal guardian's consent to the posting of children's images on social platforms, it has been pointed out in scholarly analyses, that these types of situations impose the clarification that, if photos are taken at the birthday parties that take place in the playgrounds, it will not suffice for the organizer to obtain the consent of the parents of the child who is being celebrated, yet will have to obtain the consent of all the other legal guardians of children who appear in the photos that the organiser (the services provider) intends to use for advertising and publicity purposes [21], [22]. The assent may be requested in advance or post-event; yet, it remains mandatory to collect this type of assent prior to the posting of images. Similarly, the publication of photos of other children, by a parent, on social networks, should be done only after the latter obtains, in advance, the consent of all the other parents/legal guardians. To the extent that the posting is made in the absence of the specified consent, should there be a parent who requests the removal of the child's image, the parent who posted the images must comply with the request. Otherwise, the controller will be expected to delete the images and to compensate the parties the privacy interests of whom has been compromised [3].

The need for recalibrating the transparency exigencies incumbent to data controllers, to adapt these exigencies to the particularities of children's level of understanding the risks and reverberations of personal data exposure on digital platforms has been accentuated by previous scholarly work [29]. Concerning the validity/invalidity of implicit (tacit) consent to the use of minors' personal data (including in cases in which the data controller invoked reasons pertaining to journalistic freedoms), several jurisprudential benchmarks were proven to be pertinently set, establishing the need for expressly-emitted consent, in hypotheses where the risks for prejudicial effects on the child's legal interests arose [23], especially in terms of respecting privacy preferences [30].

Along with the concerns for lack of transparency, the use of profiling techniques generating derived data while using as a primary source behavioral information collected from children (in the case of digital services targeting children under 16 as main users), may be identified as a pivotal risk, thus rendering more salient the need for imposing on the data controllers specific obligations, such as the duty to 'relational disclosure', implying the obligation to disclose to the users, prior to the collecting of their consent to data processing, the manner in which certain (potentially) disequibrated general clauses have been

accepted/rejected during a selected period of time; as emphasised in specialised literature [31], these aspects render ‘relational disclosure’ (the peer-to-peer evaluation of certain disequibrated clauses, based on previous consumer choices) even more stringent [31]. We believe that, for consolidating the level of protection when collecting children’s over 16 years old assent to the use of private information processing techniques, ‘relational information’ disclosure would be useful, by ensuring an indirect link with other consumers. The latter would be more attentive and cautious in making decisions should it was signalled to them, for example, through online banners, the problematic aspects noticed and contested by other consumers or even the highlighting of an acceptance/refusal percentage (for example, consumers should be presented, prior to requesting their consent, a message in which they are warned that ‘This clause has been accepted by 32% of consumers in the last 3 months’). We therefore believe, especially in the perimeter of younger users, between 16 and 18 years old, that it is effective for the data subject to know how other consumers (for instance, adult consumers) have reacted to the B2C (problematically imbalanced) clause [27]. Specifically, it might be saliently relevant to disclose the history of the choices of average previous consumers, in order to ensure that minor under 18 years old would be able to analyse, compare and accept or reject the general terms and conditions, in full knowledge of the case and by referring to the factual reality, considering that the latter need to be sufficiently informed, understanding not only the literal meaning, but also the core meaning of the accepted terms [29]. Nevertheless, the numerous nuances revealed when collecting the data subject’s assent [32], as well as the several progressive stages for consenting to the processing operations on which the data subject may be embarked when contracting online [33], are calling for the exposing of regulatory disquietudes which became characterizable as ‘intrinsic’ to the subject of children’s data protection [34].

Finally, it is worth mentioning that an adequate digital literacy, although highly important and extremely vital, does not necessarily result in the responsibility to mitigate against these risks being placed on the shoulders of children, in their capacity of social platforms users, especially in terms of correctly evaluating the risks associated to privacy breaches and excessive data exposure [35].

### **2.3 Legal nuances of the data controllers’ obligation of verifying the source of (parental) consent**

In the case of minors, giving consent is even more problematic, due to the inherent intricacies in terms of establishing adequate control mechanisms for verifying the expressing of the parent/legal guardian’s consent to data processing, for minors under 13 years old (respectively, for minors under 16 years old, under current Romanian legislation), to the extent that the consent cannot be considered validly given by the minor, the latter being deprived of the capacity to make valid decisions, thus the agreement will have to be collected from a person with parental responsibility. Practically, the solution to these problems consisted in transferring the responsibility from the child user to the parent. The last-mentioned aspect plays a decisive role in the protection of private information and privacy of minors, although often they are unclear when making decisions about their own personal information; yet, even in these circumstances, the right of the minor to withdraw his/her consent becomes incidental as soon as the age limit for legal competency is reached. GDPR imposes on the controllers an obligation of diligence to verify whether the holder of the parental legal responsibility of the parental authority has granted or authorized the granting of consent to children’s personal data processing, while adapting these exigencies to the available digital technologies. Synthesized in terms of ‘pertinent diligence’, the data controllers’ duty refers to the fact that the latter are obliged to verify not only the existence of consent, but also its source.

Reasonable processing, in terms of checking whether the user has reached the minimum age necessary to express his/her own consent or checking whether the person expressing consent genuinely acted in the capacity of legal guardian of the child/s interests, may depend both on the specific risks of the processing and on the technology used to verify the holder, respectively the consent of the parent; in most of the cases a verification by e-mail using parent/legal protector's contact data appears to suffice, although certain cases require more evidence so that the data controller can establish the existence of parental consent and the provenance of the agreement. Thus, based on the provisions of Article 7, 1<sup>st</sup> para. of General Regulation, it is worth highlighting that, if the processing is based on consent, the controller is expected to be able to demonstrate that the assent to the use of children's data processing techniques originated in parents or legal guardians freely expressed intent. The pertinency of the techniques used by the data controller when establishing child user's age or the recording of email correspondence between the controller and the parents are usually considered to be decisive in litigious contexts.

### **3 Particularities and incidental features of the collector's duties when processing children's data**

Several features are used to describe the substantial sphere of incidence of the precautionary measures the selection of which is incumbent on the data controller in hypotheses in which the latter intend to process private information on under-age users, especially those precautions resulting from Recital 38 GDPR, according to which:

(i) the collecting of parents' consent remains a necessary task in cases in which private information collecting techniques are intertwined to the direct offering of digital services to users under 16 years old (respectively, to users under 13 years old in EU member-states where the national legislator reduces the time bars); for other types of services (not targeting under-age users), the data collector may resort to one of the other five fundamental choices extracted from the provisions of Article 6, par. (1), letter b) to f) of the GDPR for offering legal basis to data processing operations (for instance, the performance of contractual obligations may be selected as a legal basis for private information processing, even in cases in which the *in fact* user is a child under 16, since the service was not directly targeting under-age users);

(ii) exceptions are admissible to the above-mentioned rule in cases where the data controller, who is acting in its capacity of service provider, directly targets child users, yet the nature of the service is exempt from the supplementary (mandatory) precautionary measures, namely the service provider is offering the child preventive counselling or other type of specialised advise as a type of autonomous services targeting young users and adolescents; in these hypotheses, the recording of the holder of parental responsibility' assent would not be compulsory for the data collector / the service provider;

(iii) the types of processing operations which necessitate a higher degree of precaution for the data controller, in terms of adequacy of measures selected for ensuring the respecting of parents' choice, include the processing of private information on children serving to further elaborate personalised marketing announcements to further generate user behavioural profiles the finality of which is represented by the recourse to personalised commercial advertising; in these cases, which particularly imply the constant monitoring of the child's or adolescent's behaviour and preferences in order to create a potential profile, collecting parent's consent necessitates particular attention from the service provider; for users between 16-18 years old, when private information is processed for profiling purposes, the transparency principle and the use of clear language represent the major provocative aspects that the data collector is expected to address;

(iv) when addressing the transparency issues, it is worth noticing that, in hypotheses where the private information processing concerns a child's data, and the service providing

was directly oriented towards children or adolescents, as users, there is a specific obligation incumbent on the controller, namely the duty to resort to transparent terms, formulated in plain language adapted to children's capacity of understanding, while avoiding extra-technicality or hyperabundant information, as specified in Recital 58 GDPR;

(v) the exercising of the data subject's right to oppose to further processing of private information and the subjacent right to obtain erasure of the processed data (namely, 'the right to be forgotten') is impregnated with special valences when the data subject consented to the use of the data during childhood or during adolescence, not being completely and accurately aware of the legal implications of his/her assent, as emphasised in Recital 65 GDPR.

When services addressed mixed audiences (users enrolled in different age groups), while the transparency information incumbent on the data controllers is concerned, it remains important to incorporate clear, non-abundant and easy to absorb information, using a language that is sufficiently simple for individuals in different age groups to easily digest and comprehend. Facilitating children's acquaintance to data protection and privacy rights, and familiarizing young users to accessible information may involve examples on the previous manner personal information has been used [36]. When granularity of choices is concerned, as well as the granular exercise of control over personal data, data controllers are expected to accurately describe the manner under which children may resort to data control prerogatives, namely the exercising of the withdrawal right or of the right to object to further processing, right to obtain confirmation on data storage and the soliciting of data portable formats or data erasure requests [11].

Avoiding opaque phraseology remains crucial when addressing minor's capacity of understanding pieces of information on personal data storage and data controllers are expected to adapt consistency of informative measures to the evolving capacities of the child [36].

#### **4 Precautionary addressing of automated decision making concerning a child**

The data controller's recourse to automated decision-making techniques (ADM) when using a child's data is restricted on grounds of the best interests of the child, as specified in Recital 71 GDPR; decisions made by solely using automated means without any human involvement, and profiling of child's preferences (profiling operations integrated in an automated decision-making process or, conversely, autonomous profiling operations) are raising issues of legitimacy; automated processing of personal data to gain a certain level of predictability for future conduct and future commercial choices, when the targeted individual is a child, represent major concerns in discussing the pertinency of security measures and the adequacy of transparent information delivered to the data subject. Using algorithms to make decisions concerning a minor, to predict a minor's behaviour or to control a minor's access to a digital service necessitates the implementing of data security measures every time IA techniques involve drawing inferences from the minor's previous preferences; these aspects become salient especially when using on-by-default settings, or failing to implement adequate transparency or 'by-design' safeguards (preventing child exploitation or abuse online), or using behaviour-assessing techniques which are not in 'the best interests of the child'.

#### **5 Selecting adequate measures of collecting the legal guardians' assent**

In terms of assessing the lawfulness of processing, in cases when the data controller intended to rely on 'legitimate interests' for justifying the processing of children's data as stipulated

in Article 6, 1<sup>st</sup> par., letter f) GDPR, thus arguing that the processing operations were indispensable for reaching specific purposes of the legitimate interests pursued by the data controller or pursued by a third party, the legitimacy of the processing will be evaluated through the prism of the balanced interests: are data controller's 'legitimate' interests overridden by the interests or fundamental rights and freedoms of the child, in the capacity of a data subject whose necessity in obtaining the protection of personal data would remain essential? What would be the most adequate matrix for the informing of the vulnerable data subject on the essential rights available under GDPR, and the special features of the exercise of pre-contractual information duties by the digital services provider? Are there distinct mechanisms describing the remedies available to the child's parents / legal guardians and addressing the subject of modifications made on the general terms of providing the digital services and digital content by the professional trader (the provisions on the latter being further scrutinized and developed, in accordance with specific exigences of transparency, as described in Article 12 GDPR)? Ostensibly, the manner under which the consent of the holders of parental responsibility over processing of children's data was obtained by the data controller may be subject to codes of conduct, should these be elaborated and adopted when intended to contribute to the proper application of the GDPR standards of transparency towards the data subjects.

Data controllers are expected to obey to specific rules regarding the age threshold for soliciting parental / legal representative consent, since the age on which the child becomes legally capacitated to decide on the pertinence of involving in personal data processing operations varies between 13 and 16 years, depending on the age limits set in each EU Member State.

Implementing age-verification measures remains crucial for data controllers when processing children's data, and these measures may take the form of selecting control questions, or designing actions for the parents / legal guardians willing to approach the invitation addressed by the data controller to give assent to data collecting. The reasonableness of taken measures by the implementing of which the data controller addressed the issues of collecting parents' consent is assessed by the considering of the efforts made towards the identifying child's age and the contacting of the legal guardian. Considering the availability of technology, data controllers are expected to identify pertinent techniques when requesting the minor to provide the parents' email or mobile contact data, thus enabling explicit assent to the minor's data collecting.

Data controllers may select as legal grounds for the running of minors' data processing operations the existence of the data subject's consent or the purpose of (objective) performing of the obligations that certain mandatory normative provisions would place on the data controller; symmetrically, it can be selected as legal grounds the fact that data processing would be indispensable for the exercise by the person concerned or on the latter's initiative, of individual rights or legal prerogatives, recognized in positive law (for instance, accessing certain social services when children are targeted). The existence of the data subject's consent (minor over 16 years old or the legal guardian's assent) could not be invoked, in these cases, as a basis for the processing, since by completing and signing the declarations regarding interest in accessing social services, the data subject does not pretend to be the issuer of a genuine consent to the further processing of data (for instance, for personalized advertising and marketing purposes).

Similar prerequisites remain incidental in the case of subsequent withdrawal of the parent / legal guardian's consent to the processing of the minor's personal data, in accordance with art. 7, 3<sup>rd</sup> par. GDPR, the data subject being able to withdraw consent to the processing of personal data without affecting the legality of processing based on consent prior to its withdrawal); subsequent processing of the minor's data remains possible if based on the

necessity of performing contractual obligations, without having the user's consent as a legal basis.

The using of collected data for performance purposes while engaging in direct marketing operations is covered by the provisions of art. 21 of the GDPR. Thus, in situations where the processing of children's personal data is aimed at direct marketing, the data subject (or the legal guardian, in the case of minors) has the right to object at any time to the processing, including to the generating of profiles, insofar as it is related to marketing operations directly targeting children; the consumer opposes to the processing pursuing direct marketing purposes, the possibility of further processing minor's personal data based on those commercial purposes ceases to be available to the data controller.

When the data controller or platform service provider decided to recourse to user age thresholds for accessing services, these mentioned disclaimers are not exempting the data controller from abiding to the under the GDPR standards in hypotheses where 'underage' users are directly targeted as data subjects [36]. For instance, under the provisions of art. 483 to 507 of the Romanian Civil Code, there is no rebuttable presumption on parents / minor's legal guardians acting in the best interest of the child (obviously, nor is a irrefutable presumption of this sort); therefore, it must be noted that organizations and data controllers may be able to process minor's data either on the grounds of child's vital interests where at stake (as in the case of situations presenting a certain degree of urgency) or on consideration of the sensitive nature and confidentiality of the minor's personal data. Data controllers might face the necessity of further processing available information on the existence of court orders relating to parental access or responsibility, shared custody etc., as to be able to assess the pertinence of the parent's choice on the legal treatment of child's data; this type of mission might involve non-facile tasks, in respect of the principle of data minimization, since the data controller would have to further collect personal data on the minor's legal guardians' prerogatives.

## **6 Processing data of vulnerable persons, particularly of children and the prerequisites: pre-evaluation of data-safety risks**

Negative scenarios on data safety would necessitate the adapting of data security measures in order to meet the safety requirements that the data subject is legitimately expecting to be met [28].

For the data controller, the electing of pertinent storage intervals, correlated to the nature of the respective data (ordinary data *versus* sensitive data) remains crucial, the storage duration of the children's personal data having to be viewed as sparingly as possible, in order not to enter in disagreement with the generic terms of the processing, postulated by the processing purposes. At the same time, the pertinent selection, with parsimony, of the purposes of processing children's data (from the angle drawn by applying the principle of 'limitation of purposes') remains central to the discussing of pertinent measures; equally important or 'vital' in this area is the establishing, by the data controller, of sufficiently and carefully calibrated measures for data storage review (for reviewing the relevance of the preservation of children's data), so that the private information can be erased or deleted or, depending on the circumstances, by subject to anonymization [26]. Same parsimony should be manifested when deciding whether children's data would be subject to pseudonymization, and to the using of decrypting keys as means to reestablish the identifying functionality of processed data. In the perimeter of processing operations concerning children's data, a processing operation may be considered by the data controller as being "likely to result in a high risk", thus necessitating an ex-ante evaluation carried out by the data controller or on the latter's behalf, meant to assess the likelihood of occurrence for the major scenarios of

data security breaches and the appropriateness of protocols established to manage these types of risks.

Running an *ex-ante* Data Protection Impact Assessment (DPIA) impacts the manner of selecting adequate means of processing, as well as the excluding or the including of purposes of processing on the list of purposes set by the data controller when deciding on the finalities and the duration or time bars for the collecting and the storage of personal information concerning children as data subjects.

Congruently, as specified in Recital 76 of the RGPD, the *ex-ante* assessment of the risks associated with the processing of minors' data would involve the granularization of processing operations or their regimentation by risk categories, starting from those that would present minor risks or medium risks and up to operations that would be likely to generate a high risk for the fundamental freedoms of the individuals targeted by the respective processing or would present a considerable risk of data exploitation with discriminatory effects; such a probability should be highlighted in the *ex-ante* evaluation reports or in the internal risk management protocols, implemented by the data controller prior to the start of minors' data collection and data storage procedures.

In hypotheses when children's data are subject to collecting operations, the defining of clear, non-evasive purposes of the processing operation should remain the aspect around which the processing operations will pivot, given that the requirement of proportionality of personal data processing expresses the necessity for an indispensable link between the objectives pursued by the data controller (especially, when marketing strategies targeting minors are used) and the means employed to achieve these objectives; such interference risks being qualifiable as exorbitant or disproportionate by reference to the principle of minimization of processing or to the commands deriving from the exigencies applicable to the processing of children's data, so as not to endanger privacy components.

Verifying users' age for emitting digital consent necessitates carefully calibrated strategies (by design and by default), while parents questioned on the pertinency of such verification measures previously "referred to neutral age gates used in conjunction with a second validation methodology while others emphasized that age gates should be designed to avoid 'back buttoning' and re-entry of dates of birth" when describing the spectrum of methods available to data controllers [36]. Intrusiveness of age-verification methods represent another vividly debated topic, since data controllers would manifest the tendency of over-loading information on the assessing of digital consent [36].

Further discussing points may address the issue of managing situations when the children declare to be under 16, in which case data controllers might consider implementing appropriate measures, such as zero collection of personal data during the minor's online session and the using of appropriate filtering (for listing search results) until parent's or legal guardian's consent is properly obtained [36]. Importantly, further expanded use of minor's personal data that where initially collected for limited purposes would be considered incompatible with the 'purpose-limitations' principle as described in art. 5, 1<sup>st</sup> par., letter b) of the GDPR, the respecting of which is incumbent on data controllers. Such prerequisites are equally important for data controllers intending to extrapolate initially selected data processing purposes, as to incorporate further processing purposes concerning child's personal information, as for offering personalized advertising messages and marketing-oriented profiling techniques which would involve the processing of children's data [37]; data controllers might be held liable for transgressing the precautionary regime applicable to the processing of 'under-age' users' personal information as 'derived data' (from the taxonomy of profiling operations). Requesting consent to the receiving online direct marketing communications targeting adolescents and children is subject to the 'granularity' and 'specificity' standards described in art. 4(11) GDPR on the definition of 'consent' and art. 7 GDPR on conditions for consent validity; yet, the peculiarities of young users' limited

life experience must also be considered when calibrating consent collecting methods; importantly, assent to direct marketing communications can only be collected from individuals over 16 years, otherwise, parents 'consent becomes indispensable for further processing of these types of personal information. Users' right to object to the processing of data for direct marketing purposes will also activate in such cases, according to art. 21, 2<sup>nd</sup> and 3<sup>rd</sup> par. GDPR and to Recital 70 GDPR.

## **7 Sensitive data collected from children**

The processing of sensitive data is subject to considerably stronger rigors and demands than those generally incident to the processing of usual personal data, hence the importance of a *reductio ad minimum* practiced in the perimeter of this category of processing. The peculiarity which makes processed personal information to be categorized as 'sensitive', selected from the category of 'usual' or typical personal data, as a special category, is the aptitude, ostensibly more accentuated, in these cases, to endanger the privacy rights of the data subjects, uncovering elements of their private life that could make them significantly vulnerable, subsequently placing them in the position of potential victims of discriminating decisions, damaging their reputation, facing professional/social marginalization or damaging social relations, as facts facilitated by third-parties accessing 'sensitive' information [34]. As resulting from Recital 75 GDPR, in the perimeter of processing children's sensitive information, particularly medical information and data relating to health pathologies, the severity of the privacy risks associated to these types of data processing becomes significantly higher than in the case of adults consenting to the use of their medical data.

In the context of conducting the risk assessment for the processing of children's sensitive personal data, namely for the profiling based on the processing of sensitive data which may have potential negative effects on the data subject's privacy rights, it renders necessary the selection of sufficiently pertinent and adequately tailored guarantees, while the establishing of legal remedies available to the data subject for the legal rebalancing of the privacy prerogatives remains crucial. When processed, personal data whose nature, intrinsically, implies the existence of potential risks for privacy rights, will require the selecting, by the data controller, of internal protocols regarding data processing, which allow specific protection, based on the desirability of preserving their integrity in the face of malware-type attacks or other types of security breaches, since minimizing the importance of processing could generate considerable risks to privacy rights. Similarly, it is important to highlight that either the data controller or the persons authorized by the latter are required, in imperative terms, to establish appropriate guarantees, in a consistent manner, in addition to the usual organizational measures, considering the heightened level of risks associated with the processing of children's sensitive data; thus, on a first level, the measures aimed at minimizing the amount of processing data or reducing the categories of processed data would have to be implemented accordingly to the meta-rule bearing the desiderata of minimizing the processing of personal data; for concentric reasons, it remains vital, within the perimeter of sensitive data processing, to employ technical or organizational measures aimed at ensuring that the data controller respects the principle of the integrity of the processed data, respectively the principle of the confidentiality of the processed data [35].

As postulated in the text of art. 9, 1<sup>st</sup> par. GDPR, the data controller is placed under a ban on processing data from the categories of 'sensitive' personal information, which would have the potential to be exploited in a discriminatory manner or could, in other ways, alter the exercise of fundamental freedoms; included in these categories are the data that reveal the political, trade union or religious options of the individuals, respectively their sexual orientation; on another level, the processing of genetic data and, similarly, those that exploit biometric data (being targeted, however, only biometric data exploited for the purposes of

identification/establishing the identity of natural persons), respectively data that reveal aspects regarding the health status of the individuals [34].

As outlined in Recital 75 of the GDPR, the data controller's failure to assimilate additional security measures for the treatment of sensitive data, the failure to conduct or the improper conduct of the *ex-ante* impact studies on the potential risks which are located on different levels and presenting differentiable gradients, in terms of the extent and in terms of the probability of occurring, and which the processing of sensitive data could generate for fundamental freedoms, as well as slippages in maintaining the records of sensitive data processing (especially through the prism of the prohibition aimed at their non-selective processing) represent culpable behavior (impermissible actions or omissions); such actions/omissions of the data controller may generate either physical (bodily, biological) damages to the minors whose sensitive data were subject to improper processing, or emotional damages, being listed as examples of the categories of situations in which such risks inevitably affect the minor's rights, the sensitive data of whom was subject to processing, both in online and offline contexts.

Listed in Recital 75 of the GDPR are also the situations of processing by operators of minors' data or of sensitive information collected from other vulnerable categories through the prism of age or the absence of life experience that would suffice when estimating the risks associated to the data collecting. The last on the list of situations that fuel high levels of risk regarding the processing of personal information are the cases in which the processing (of sensitive data) is extensive from a quantitative or volumetric point of view, involving consistent amounts of processed data (even if coming from a limited number of minors, in their capacity of users of digital services).

## 8 Conclusive Remarks

Seen as a genuine 'cornerstone' in the legal architecture of data protection, the legal mechanism of consent withdrawing to data processing is directly connected to the fulfilment of the obligation incumbent on controllers in terms of informing the parent (in the latter's capacity of adult guardian of the child whose data are collected and processed) regarding the existence and the ways of exercising this faculty of consent retract. Consequently, the approach of the gradients of good faith in the execution of the (pre-contractual and/or contractual) obligation to inform becomes indispensable to discern the contours, not necessarily volatile, but certainly versatile, of withdrawing data subject's consent in contracts formed on virtual platforms.

The General Regulation preserves the possibility for Member States, through the adapting of national law, to opt for regulating a lower age for children's data processing purposes, of at least 13 years, and imposes on controllers the obligation of verifying in such cases that the parent has granted or authorized consent, while considering the particularities of available technologies. Therefore, after reaching the digital age, at 16 years at the latest, children themselves become responsible for the content they post on social networks, thus rendering the 'granularity of consent' exigencies even more stringent.

Addressing the issue of the 'granularity of consent' in terms of collecting and processing children's data, there is a miscellany of convergent and non-convergent answers, hence the importance of methodical approaches and of the practitioner's commitment to use clear legal mechanisms. As a rational secondarily derived argument, the necessity for a clear and unambiguous action, resulting in parent's granularly obtained assent becomes even more stringent in the perimeter of the protecting of children's data, especially on social networks, but, more largely, in B2C relationships involving personalised advertising based on profiling. Legal answers to these key issues are invariably imbued with references to the discretionary

nature of the assent, namely the adult guardian/parent's decision concerning the processing of under the age of 16-child's data.

Specifically, the solutions to the interrogations on the respecting of the 'granularity of consent' principle, more stringently in the sphere of collecting children's data, are inspired or permeated with references to the general rule according to which, for any processing of children's images in an educational context or entertainment services addressed to children under the age of 16 (or 13 years old, in member-states in which the national legislator opted for lowering the time frame to 13 years old), the consent of the parents or representatives of the parental authority is required, regardless of whether the images are posted on social networks by the employer who organized the event or by the third party who took part in the event, such as the owner of the playground, suppliers or party entertainers, during educational events meant to promote children-addressed products or services.

Finally, in terms of assessing the absence of the elusive effect on civil liability for the prejudicial processing of children's data, it is worth emphasising that precautionary measures on parents' consent collecting become non-compulsory for the data controller in situations where the service provider is offering the child preventive counselling or other type of specialised advise, and these types of autonomous services were targeting young users and adolescents; in these hypotheses, the recording of the holder of parental responsibility' assent would not present a mandatory nature for the data collector / the service provider.

## References

1. D. F. Barbur, *Protecția datelor cu caracter personal*, 2nd edition (C.H. Beck, Bucuresti, 2002)
2. J. Goicovici, *Analele Universității de Vest din Timișoara, Seria Drept*, **2**, 7-24 (2019)
3. D. F. Barbur, *Pandectele Române*, **5**, 63-72 (2021)
4. L. Archbold, D.- Clifford, M. Paterson, M. Richardson, N. Witzleb, *University of New South Wales Law Journal*, **44(3)** (2021)
5. M. Arenas Ramiro, A. Ortega Giménez (eds.), *Tratamiento de datos personales en centros educativos. Cuestiones prácticas*, (Editorial Sepin – Servicio de Propiedad, Madrid, 2021)
6. S. Grimes, *EDPL*, **8(1)**, 14-18, DOI: <https://doi.org/10.21552/edpl/2022/1/5>. (2022).
7. J. Dolan, *EDPL*, **8(1)**, 7-13, DOI: [10.21552/edpl/2022/1/4](https://doi.org/10.21552/edpl/2022/1/4) (2022)
8. J. Goicovici, *Dreptul relațiilor dintre profesioniști și consumatori* (Hamangiu, Bucuresti, 2022)
9. J. Goicovici, *Revista Română de Drept Privat*, **1**, 304-328 (2022)
10. J. Henrich, *EDPL*, **5(1)**, 78-79, DOI: [10.21552/edpl/2019/1/12](https://doi.org/10.21552/edpl/2019/1/12) (2019)
11. J. Goicovici, *Analele Științifice UAIC, SSJ, Tomul LXVII/2*, 57-80, DOI: [10.47743/jss-2021-67-4-4](https://doi.org/10.47743/jss-2021-67-4-4) (2021)
12. J. Goicovici, *Revista Română de Drept Privat*, **2**, 399-415 (2019)
13. R. Gola, *Droit du e-commerce et du marketing digital* (Gualino, Paris, 2019)
14. S. Van der Hof, S. Ouburg, *EDPL*, **8(1)**, 61-72, DOI: [10.21552/edpl/2022/1/10](https://doi.org/10.21552/edpl/2022/1/10) (2022)
15. I.-F. Popa, *Revista Română de Drept Privat*, **1**, 153-184 (2018)
16. E. Kaiser, *EDPL*, **6(4)**, 607-610, DOI: [10.21552/edpl/2020/4/19](https://doi.org/10.21552/edpl/2020/4/19) (2020)
17. E. Lievens, *EDPL*, **7(3)**, 423-428, DOI: [10.21552/edpl/2021/3/11](https://doi.org/10.21552/edpl/2021/3/11) (2021)

18. I. Milkaitė, R. De Wolf, E. Lievens, T. De Leyn, M. Martens, *Children and Youth Services Review*, **129**, DOI: 10.1016/j.childyouth.2021.106170 (2021)
19. M. Macenaite, E. Kosta, *Information & Communications Technology Law*, **26(2)**, 146-197, DOI: 10.1080/13600834.2017.1321096 (2017)
20. N. Martial-Braz, J. Rochfeld, *Droit des données personnelles. Les spécificités du droit français au regard du RGPD* (Dalloz, Paris, 2019)
21. F. Mattatia, *RGPD et droit des données personnelles, Fifth edition* (Eyrolles, Paris, 2021)
22. M. Maxim, *Răspunderea civilă contractuală în domeniul protecției datelor cu caracter personal în contextul noului Regulament general (UE) privind protecția datelor 2016/679*, (Universul Juridic, Bucuresti, 2021)
23. E. Politou, E. Alepis, C. Patsakis, *Journal of Cybersecurity*, **4(1)**, 5-18 (2018)
24. K. Poludniak-Gierz, *European Review of Private Law*, **26(3)**, 297-309 (2018)
25. OECD, *Children in the digital environment: Revised typology of risks*, OECD Digital Economy Papers No. 302, OECD Publishing, DOI: 10.1787/9b8f222e-en (2021)
26. OECD, *Protecting children online: An overview of recent developments in legal frameworks and policies*, OECD Digital Economy Papers No. 295, OECD Publishing, DOI: 10.1787/9e0e49a9-en (2020)
27. \*\*\*, *Limits to Journalistic Freedom in Reproducing the Image of a Hospitalized Minor – Italian case law* *Journal of European and International IP Law – GRUR International*, **71(1)**, 82-87, DOI 10.1093/grurint/ikab132 (2022)
28. A. Davola, I. Querci, S. Romani, *No Consumer is an Island – Relational Disclosure as a Regulatory Strategy to Advance Consumers Protection Against Microtargeting*, SSRN, DOI: 10.2139/ssrn.4068548 (2022)
29. M. Dumitru, C. Pristavu, *Revista Română de Drept al Afacerilor*, **1**, 26-49 (2021)
30. M.-C. Dobriță, *Analele Științifice UAIC. SSJ*, **LXVII, Supplement**, 211-225, DOI: 10.47743/jss-2021-67-3-15 (2021)
31. P. Borzykh, *Concept of Personal Data in Social Media Environment: Effect of General Data Protection Regulation and Trade Secrets Directive*, SSRN, DOI: 10.2139/ssrn (2021)
32. G. Buttarelli, *EDPL*, **3(2)**, 155 – 159, DOI: 10.21552/edpl/2017/2/5 (2017)
33. A. Vogel Y, *EDPL*, **8(2)**, 238-249, DOI 10.21552/edpl/2022/2/10 (2022)
34. J. Goicovici, *Studia Universitatis Babeș-Bolyai Iurisprudentia*, **67(4)**, 13-54, DOI: 10.24193/SUBBjur.67(2022).4.1 (2022)
35. T. Tombal, I. Graef, *The regulation of access to personal and non-personal data in the EU: from bits and pieces to a system?*, SSRN, DOI: 10.2139/ssrn.4304148 (2022)
36. Data Protection Commission (DPC), *Fundamentals for a child-oriented approach to data processing* (Dublin, 2021)
37. J. Goicovici, *InterEULawEast: Journal for the International and European law, economics and market integrations*, **9(2)**, 43-68, DOI: 10.22598/iele.2022.9.2.2 (2022)