SMART INFERENCE-DRIVEN RISKS: LEGAL CHALLENGES UNDER THE GDPR AND THE EGYPTIAN PDPL

Esraa HASHISH

Assistant Professor of Civil law,
Faculty of Law, Alexandria University, Egypt[1]
E-mail: dr.esraa.hashish.law@alexu.edu.eg

Abstract

This paper examines the legal dilemma surrounding inferences about sensitive data and how the EU General Data Protection Regulation (GDPR) and the Egyptian Personal Data Protection Law (PDPL) treat such inferences as sensitive data. Using doctrinal research supported by a review of the jurisprudence of the Court of Justice of the European Union (CJEU) [2], this study explores how both frameworks address the protection of inferred data. This analysis reveals significant overlap in the definitions of personal and sensitive data, confusion over consent requirements in Egypt, and heightened risks of discrimination arising from inferred data. Moreover, the existing risk assessment mechanism is insufficient to produce a protection for the inferred data and indicates the necessity for an impact assessment akin to that of the GDPR. This study addresses a proposed framework for the Egyptian legislature and courts for the inferred data that could be assessed through the risk criterion, the data subject's rights with inferences, and the controller and processor's transparency obligation. Furthermore, the paper argues that recognition of such inferences as sensitive data is globally essential for ensuring stronger safeguards in the era of AI and big data and addresses global lessons for other jurisdictions that have not yet recognized sensitive data.

Keywords: *Privacy, Personal Data, Sensitive Data, Inferences, GDPR, PDPL, Egypt*

---

[1] ORCID iD: 0009-0003-1693-8415.

[2] Case C-394/23 (2025), C-252/21 (2023), C-446-21 (2024), C-184/20 (2022), C-21/23 (2024), C-667/21 (2023), and C-136/17 (2019).

1. Introduction

All privacy laws deal with "personal data" due to a natural person's fundamental right to privacy and protection during the processing of data (*GDPR*, 2016), which is required for big data (*EU Data Act*, 2023), whether involving personal data or sensitive data, throughout the various phases (Kumar et al., 2024, pp. 18- 22; Soria-Comas & Domingo-Ferrer, 2016, p. 22) until the data is published or shared (Jain et al., 2016, p. 2; Wanjale et al., 2021, p. 103). This right is also required during the entire lifecycle of the AI system in accordance with its non-binding ethical principles (*EU AI Act*, 2024).

Due to uncertainty and the definitional overlap about when data is personal and when it is not (Rupp & Von Grafenstein, 2024, p. 105933), inferred data, or inferences about sensitive data, require a high level of protection as sensitive data. Furthermore, personal data could lead to the revelation of special data, the disclosing of which could lead to a significant risk to the data subject and his/her fundamental rights.

The CJEU concludes that inferences derived from personal data should be considered sensitive data; however, the Egyptian PDPL *(PDPL,* 2020*)* does not explicitly recognize inferences. In the author's view, inferred data should receive the same level of protection as sensitive data based on the risk criterion.

It is the author's belief that Egypt's forthcoming executive regulations—which have not been enacted to date—should recognize inferences as sensitive data where they reveal sensitive information, and other special data, which are not classified as sensitive but the revealing of which could cause serious harm to individuals, should be protected as sensitive data.

The author presents the gap in the Egyptian law, as the law does not provide protection for inferences about sensitive data, and how Egypt's forthcoming executive regulations and courts should address inferences, and which should be assessed upon the risk criterion. With the risk criterion, the author addresses the PDPL's risk assessment. Furthermore, the author presents how sensitive data and inferences are not globally recognized in all jurisdictions, highlighting a manifested imbalance in data protection laws.

This paper will explore both laws, GDPR and PDPL; the definition of personal and sensitive data; how the legislatures create confusion through their drafting of laws; how relevant judgments of the CJEU deal with these inferences; and how Egypt and other jurisdictions regulate such inferences.

2. Research Methodology

This research primarily adopts the doctrinal, comparative, and jurisprudential methods in legal studies, which rely on literature interpreting the General Data Protection Regulation (EU GDPR), the Egyptian Personal Data Protection Law (Egyptian PDPL), and other related legal sources such as the guidelines of Article 29 of the Data Protection Working Party and interpretations of the Egyptian PDPL by scholars and other secondary textual sources.

This study adopts the comparative approach and the statutory analytical approach by comparing the laws of the European Union with those of Egypt and focusing on the boundaries of personal and sensitive data, the requirement of consent for lawful processing, the treatment of inferred data, and children's data. This leads to the author's proposals for Egypt regarding a new boundary based on the risk criterion of data and a new framework for inferences. Finally, the research adopts a jurisprudential analysis and reviews relevant judgments issued by the Court of Justice of the European Union (CJEU) (Nguyen et al., 2025, p. 19; Snyder, 2019, p. 334).

Table 1 Legal Sources Examined in This Study and Axes of Comparison

Source: The author

Sources examined	**Axes of Comparison**	**Comparative Analysis**	**Proposal for Egypt's PDPL**
• Primary sources ⇒ (Legislative Texts: (GDPR, PDPL). ⇒ Regulatory& Jurisprudential Sources: (Art. 29 (WP), EDPB Guidelines, CJEU case law). • Secondary sources ⇒ Academic Commentary.	• Definition of personal and sensitive data. • Lawfulness of data processing. • Treatment of inferences. • Children's data.	• EU GDPR • Egypt's PDPL	The boundary between personal and sensitive data Risk criterion

3. Research Results and Discussion

3.1 Personal and Sensitive Data in the GDPR

While the GDPR uses the terms "personal data" and "special categories of personal data," the United States named them "personal information" and "sensitive data" in the CCPA *(CCPA, 2018)* and the CPRA *(CPRA, 2020*; Widjaja, 2024, p. 789), taking into account that the terms "personal data" and "sensitive data" might differ within federal and state laws. (Solove, 2023, p. 1085, fn. 4; Solove & Schwartz, 2019, p. 1255).

Although the GDPR is considered the most protective regulation in the field of data protection (Voss, 2021, p. 7), the GDPR's basis of such classification of data relies on the nature of the data, in contrast to the CJEU, which ruled in C-667/21 that "EU legislature assumes … processing of personal data may be a source of risk …" (*Medizinischer Dienst der Krankenversicherung Nordrhein*, 2023, para. 98), which aligns with the author's belief that the base of these classifications should be the risk and is supported by recitals 75 and 77, which provide that "The risk … may result from personal data processing … lead to physical or non-material damage …."

A. Definition of personal data:

a) Data relating to an "identified or identifiable" individual

GDPR defines personal data in Art. 4 (1) as "Any information" that relates to an identified or unknown identifiable natural person, making that person identifiable, either directly or indirectly, when accompanied with other data. And this marks the beginning of recognizing the power of inferences.

b) Types of personal data

The term "any information" is a flexible term that could include a wide range of information that could be linked to a natural person, such as the data subject's name, an online identifier such as an email address, or a financial account (*CPRA*, 2020, Section 140), and other factors that make his/her identity "identified or identifiable."

For example, IP addresses are considered personal data in C-582/14 when it declared that "… only the internet service provider could connect the IP address to an identified subscriber." (*Patrick Breyer v Bundesrepublik Deutschland*, 2016, para 20, 21; *Directive of 95/46/EC of 1995*, 1995).

B. Lawfulness of Processing Personal Data:

a) Consent

The data subject's consent, which is an acceptance of an invitation directed to people to accept a data processing operation (*EDPB*, 2020, p. 5, n. 5), considers a requirement for the lawfulness of the processing of his/her data for one or more specific purposes, according to Art. 6 (1) (a), recital 32 and 40, and Art.

4 (11), and such consent must present a freely indication of will and his/her wishes and as held in C-252/21 that such acceptance may be presented through clicking on the sign up button " … users of the social network Facebook … when they click on the "sign up" button …" *(Meta Platforms and Others (General Terms of Use of a Social Network),* 2023, para 28; Gupta et al., 2024, p. 20 –27) is considered a declaration of consent.

The GDPR does not require a specific form for obtaining consent, and the handwritten signature may constitute a valid expression of consent/acceptance to processing. However, according to case C-200/23, consent can not serve as a valid legal basis where there is a clear imbalance of power between the parties, particularly when the controller is a public authority, as the court held that "… Consent should not provide a valid legal ground … where there is a clear imbalance … in particular where that controller is a public authority." (*Agentsia po vpisvaniyata v Ol*, 2024, para 100).

b) Exceptions

Although lawfulness of data processing basically requires the data subject's consent, the GDPR provides that processing is considered lawful in specific cases, such as where processing is for the performance of a contract, compliance with an obligation, protection of the data subject's vital interests, performance of a task for the benefit of public interest or in the exercise of official authority, and purposes of legitimate interests, Art. 6 (1) (b) to (f).

C. Definition of Sensitive Data:

a) Sensitive due to their nature or risk

The sensitive data provided in Recitals 10 and 51 and Art. 9 is specified data that requires a high level of protection. The GDPR provides restrictions for the processing of such data because this could result in significant risks to the fundamental rights and freedoms of individuals.

Historically, the non-binding guidelines of the Organization for Economic Co-operation and Development (OECD) on the protection of privacy and trans-border flows of personal data (Mesarčík, 2020, p. 82), provide that "it is probably not possible to define a set of data that are universally regarded as being sensitive" (Quinn & Malgieri, 2020, p. 5).

Unlike the OECD's guidelines, the Council of Europe's binding Convention no. 108 for the protection of individuals with regard to the processing of personal data which is listed as sensitive data (Quinn & Malgieri, 2020, p. 5; Kovalenko, 2022, p. 39; Turnšek & Kraljić, 2024, p. 187). An opinion suggests that the idea of sensitive data almost focuses on preventing discrimination and risks against individuals (Citron & Solove, 2021, p. 826).

One of the sensitive data debates is whether to be in an open or a closed list, which means whether to allow new types of sensitive data to be added or not. Unlike the OECD, which adopted an open list, the EU Directive 95/46/EC of 1995 (DPD) adopted a minimum open list of seven categories (*Directive of 95/46/EC of 1995*, 1995) and provided seven exceptions to such rules, and countries were able to add more types to such list.

With the GDPR, member states cannot add new categories to such a list, but according to Art. 9 (4), member states can introduce more conditions and limitations regarding the processing of specific data, which are genetic data, biometric data, or data concerning health (Solove, 2023, p. 1089).

b) The GDPR's closed list

The GDPR defines "sensitive data" in Art. 9 (1) with a closed list that determines the nature of data that its revealing is a disclosure of sensitive data and includes racial or ethnic origin, political opinions, trade–union membership, health, sex life or sexual orientation, genetic data, and biometric data.

This list indicates that although the GDPR in Art. 10 permits processing of criminal convictions and offenses under the control of official authority, "criminal records" are not listed in the GDPR's list, but they require a higher level of protection due to their legal effects on reputational status, as mentioned in C-136/17, and might lead to risks of discrimination due to their "sensitive nature" and risk of "… serious interferences with the fundamental rights …" (*GC and Others v Commission Nationale de l'informatique et des libertés*, 2019, para. 44).

In the author's view, the court combines both criteria when it declared that "… excluded … the activity of a search engine from … those provisions for processing relating to the special categories of data referred to there would run counter to the purpose of those provisions … because of the particular sensitivity of the data, is liable to constitute … serious interference with the fundamental rights …" (*GC and Others v Commission Nationale de l'informatique et des libertés*, 2019, para. 44).

D. Lawfulness of Processing Sensitive Data:

a) General Prohibition

Article 9 (1) of the GDPR provides a "General Prohibition" on processing of sensitive data that reveals the aforementioned specified data.

b) Exceptions

Processing of sensitive data shall be considered lawful, according to Art. 9 (2), where the data subject provides his/her explicit consent to the processing, especially when there is an automated decision-making based on sensitive data (Solove, 2022, p. 1030), for carrying out obligations, to protect vital interests, for legitimate activities, where data is made public by the data subject, for a defense of a legal claim, for substantial public interest, for medical and health matters, for purposes of assessment of the working capacity of the employee, for public interests in the area of public health, and for archiving purposes.

E. Dilemma: Inferences about Sensitive Data:

A dilemma can take two main forms:

a) When the processing of personal data is based on the data subject's consent

The processing shall entitle the data subject to the right to use his fundamental rights and to withdraw his consent when processing reveals inferences about sensitive data.

b) When the processing of personal data is lawful regardless of the data subject's consent

In the author's opinion, the inferred data should be considered sensitive, as follows:

- Art. 29 (WP)

Which provides that any personal data that can reveal specified types of data should be considered sensitive data. Furthermore, the term "revealing" combines both information that is sensitive by its nature and information concerning an individual that could be inferred and that considers inference. (*Article 29 Data Protection Working Party*, 2011, p. 6).

- The GDPR

The law explicitly considers photos as personal data, but Recital 51 provides that processing of photos should be considered processing of sensitive data where the processing involves specific technical means that disclose the unique identity of a natural person, which leads to inference about sensitive data.

- The CJEU

The court, as being the authorized authority for the interpretation of EU laws, declared in many cases (Hoofnagle et al., 2019, p. 71 fn 63, 82) that personal data could result in inferences about sensitive data, which implies a higher level of protection as sensitive data, as follows:

I. Gender Identity:

Although the CJEU does not explicitly classify gender identity as 'Mr.' or 'Ms.' as sensitive data, the CJEU held in Case C-394/23 that this identity could indirectly disclose sensitive data, as the processing of personal data relating to the title "male or female" of the customers could reveal the risk of discrimination on grounds of gender identity (*Mousse v Commission nationale de l'informatique et des libertés (CNIL) and SNCF Connect*, 2025, paras 13 & 71 (1) (point 2 & 5)).

II. Social Media Account:

CJEU held in C-252/21 that "… processing of personal data from visits to websites or apps …" *(Meta Platforms and Others (General Terms of Use of a Social Network),* 2023, para 73), which are collected by an online social network, are considered personal data if the data could make the user's identity identified or identifiable. When one or more types of sensitive data are related to these visits or apps, the processing of such data from visits to these websites, linking that data with the user, must be regarded as sensitive data "… where that data processing allows information falling within one of those categories to be revealed …" (*(Meta Platforms and Others (General Terms of Use of a Social Network)*, 2023, para 155 (2)).

III. Processing a data subject's other data obtained via third-party websites and apps:

CJEU held in C-446/21 that although the data subject "… made a statement about his/her sexual orientation in a discussion open to the public, does not authorize the operator … to process other data relating to the person's sexual orientation, obtained … outside the Meta platform using third-party websites and apps …" *(Maximilian Schrems v Meta Platforms Ireland Ltd*, 2024*, Para 84 (2)),* as the collection of these other data results in inferences "… which could be drawn from his friend list …" *(Maximilian Schrems v Meta Platforms Ireland Ltd*, 2024, Para. 24) with other sensitive data.

IV. Content of Declarations of Private Interests:

CJEU declares in C-184/20 that the publication on the website of the public authority of some personal data, such as the names of public officials' spouses or partners, could indirectly reveal sensitive information, such as sexual orientation, that could lead to serious inferences about sensitive data: "… are liable to disclose indirectly the sexual orientation … constitutes processing of special categories …" *(OT v Vyriausioji tarnybinės etikos komisija (Lithuania)*, 2022, para. 129 (2)).

V. Customer's Information when Ordering Medicinal Products Online:

CJEU held in C-21/23 that "… where the data on purchases of medicinal products allow conclusions to be drawn as to the health status … they must be regarded as data concerning health." *(ND v DR*, 2024, para 87). As "… for personal data to be classified as data concerning health, … are capable of revealing information about the health status of the data subject by … collation or deduction" *(ND v DR*, 2024, para. 83), and the identity of the data subject becomes identified or identifiable, allowing the deduction of his/her health status.

F. Definitional overlap in other global jurisdictions:

Other jurisdictions vary in regulating data, from recognizing inferences from personal data to not distinguishing between personal and sensitive data, as follows:

a) In the United Kingdom:

The UK's Data (Use and Access) Act (DUAA) 2025 *(Data Use and Access,* 2025*)* does not define sensitive data, contrary to the Data Protection Act 2018 *(UK Government,* 2018*),* the UK GDPR, and the highly persuasive, though non-binding, guidance of the Information Commissioner's Office (ICO). The ICO guidance recognizes sensitive data as either "factual or inferred" information about a person and affirms that inferred data requires the same high level of protection as directly collected sensitive data. Furthermore, the guidance clarifies that where there is an intent to infer or to act differently based on inferences, the inferred data should be considered sensitive data *(UK,* 2024a*; UK,* 2024b*; UK,* 2024c*).*

b) In the USA:

Both the California Consumer Privacy Act (CCPA) *(CCPA,* 2018*)* and the California Privacy Rights Act (CPRA) (*CPRA*, 2020) explicitly, in Section 14, §§798.140 (V)(1)(K), recognize the notion of inferences as a form of personal data, which provides that "inferences," or "derived data," means information derived from the consumer's other personal data reflecting the consumer's preferences, characteristics, behavior, or attribute, and it would be inconsistent for California law to recognize inferences about personal data but not recognize inferences about sensitive data (Solove, 2023, p. 1102).

Moreover, the Colorado Privacy Act (CPA) 2023 *(CPA,* 2023*)* explicitly, in §904-3-2.02, defines "sensitive data inferences" as inferred data collected by a controller—based on personal data, either alone or in combination with other data—and used to indicate sensitive data about an individual and treats such inferred data as directly collected as sensitive data.

c) In India:

The Digital Personal Data Protection Act (DPDPA) 2023, *(DPDPA,* 2023) in Section 2 (t), defines personal data to mean any information that can directly or indirectly identify an individual and does not distinguish between personal data and sensitive data. However, the law does not introduce special data named "sensitive data" and does not explicitly recognize the notion of inferences (Kohli, 2023).

d) In Canada:

The Digital Charter Implementation Act (DCIA) 2022 (Bill C-27) *(Digital Charter Implementation Act,* 2022*),* which includes the Consumer Privacy Protection Act (CPPA), recognizes inferences from personal data and treats them as personal data in Part 1 Section 9 (2). However, both laws do not explicitly define sensitive data or inferences; the law requires the organizations to consider the volume and sensitive nature of the personal data under their control. Moreover, the Office of the Privacy Commissioner (OPC), in its non-binding recommendations n. 7 & 8, defines sensitive data and suggests that the definition of personal data should explicitly include inferred data, "inferences" of personal data *(Digital Charter Implementation Act,* 2020*).*

3.2 Personal and Sensitive Data in the Egyptian PDPL

While the Egyptian PDPL is struggling with the lack of personal and sensitive data boundaries, the confusion is raised more where the PDPL provides that "personal data may not be … processed … except with the explicit consent … or where otherwise permitted by law," Art. 2 *(PDPL, 2020)* in writing where required, for processing of personal and sensitive data, and because the executive regulations, which are supposed to clarify the distinction between the two forms of required consent for processing, have not yet been enacted, in addition to the absence of relevant case law in this area until now.

A. Definition of Personal Data:

The PDPL defines personal data with a general rule, "Any data" that relates to a natural person and makes him/her identified or identifiable, and determines types of such data, such as a person's voice and picture. The data subject's geographical location is a new identification element in the UAE PDPL (*UAE Federal Decree No. (45) of 2021 Concerning the Protection of Personal Data*, 2021).

B. Lawfulness of Processing Personal Data:

a) Explicit Consent in the PDPL

Although the data subject's explicit consent is a requirement for the lawfulness of processing, the law does not provide manners in which the data subject

should present such consent (Eldomiaty, 2022, p. 31; Mahdy, 2025, p. 4312). Using analogy with provisions of the Egyptian Civil Law (*Egyptian Civil Law No. 131 of 1948*, 1948), which define valid consent (whether explicit or implied) for the formation of contracts in Art. 89 and Art. 90, the required explicit consent in the PDPL implies that the data subject should present his desire/wish or acceptance to establish the determined legal effect, which is to process his data.

Presenting such explicit consent, or "digital consent" (Mahmoud, 2024, p. 1444; Mahdy, 2025, p. 4308), could be oral, written, or by any means from which a holistic assessment of which and with the individual circumstances must find its way to constitute an acceptance (Wiedemann, 2020, p. 458) and shall eliminate implied consent, other passive forms of consent, silence, and inactivity.

b) Explicit consent in the GDPR

Using the analogy with the GDPR, which requires "explicit consent" for processing of sensitive data and does not differentiate between the nature of consent required for processing personal and sensitive data (Solove, 2023, p. 1097). "Explicit consent" in Art. 4 (11) and recital 32 of the GDPR means any freely given and unambiguous indication of the data subjects' wishes indicating "acceptance," either by written statement, including by electronic means, or an oral statement, and could include ticking a box when visiting an internet website.

C. Definition of Sensitive Data:

a) Sensitive due to their nature or risk

Although the PDPL does not provide a clear definition for sensitive data, it prohibits the processing of any personal data that reveals the listed determined data which is considered, by law, sensitive data. The PDPL provides those data with a higher level of protection, as the legislator requires in Art. 12 that "… the controller or processor must obtain the explicit written consent …" for its processing. The rationale behind that is that the misuse of such data could have risky consequences on an individual's privacy and fundamental rights.

b) The PDPL's closed list

The PDPL adopts a closed list of sensitive data, such as health, religious, and financial data, and provides a clear statement that the child's data is considered sensitive data. Sensitive data is not "sensitive" because it is sensitive information by nature, but because it will reveal what the legislator considers to be sensitive data. the author believes that such data may be inherently sensitive by nature, or non-sensitive by nature, but the disclosing of it could result in inferences about other sensitive data.

Moreover, the legislator does not provide any criteria for what constitutes a "sensitivity element" in these data, which is supposed to gather them in the designated list. Unlike the PDPL, another data protection law in Africa defines sensitive data as information that is particularly sensitive to an individual, such as health data (Staunton et al., 2025, p. 7).

Egyptian authors conclude that a closed list for sensitive data is an unproductive idea, as the legislator did not clarify why they are considered sensitive data (Ali, 2025, p. 4075). It is the author's belief that the definition of sensitive data should be redefined to include personal data or even non-personal data resulting from inferences about sensitive data. Judges should obtain wider discretion authority regarding these data that are supposed to be protected as sensitive data, especially where those data lead to an individual's serious danger and risk. (Rashad, 2024, pp. 1061, 1063, 1088, 1089, 1098).

This conclusion is supported by Art. 29 (WP), which states that individuals' photos should be considered sensitive data because they can be used to infer religious beliefs or health-related information, even though photos are not inherently classified as sensitive data. (*Article 29 Data Protection Working Party*, 2011, p. 6).

D. Lawfulness of Processing Sensitive Data:

a) General Prohibition

The PDPL in Art. 12 provides a general prohibition on controllers and processors for processing or disclosing sensitive data and processing a child's data.

b) Exceptions

The law provides the following exceptions in Art. 12 that permit sensitive data processing in specified circumstances:

- "The controllers and processors … are prohibited … except by virtue of a license issued from the Center," as the Personal Data Protection Center (PDPC), according to Art. 19 and 26 (6), is responsible for regulating personal data processing and is authorized to issue licenses for processing.
- In special determined "cases authorized by law."
- Where the "controller or processor … obtains the explicit written consent of the data subject."
- Where "… activities in relation to children's data, the guardian's consent must be obtained."

E. Dilemma: Inferences about Sensitive Data:

a) Definitional Overlap in the PDPL

The PDPL in Art. 1 considers a person's health, psychological, and financial status once as personal data and another as sensitive data, as personal data means "any data which determines the psychological, health, economic, … identity …" while sensitive data refers to "data which discloses psychological, mental, or physical health or genetic … or financial data … ," indicating that there is no clear boundary between personal and sensitive data and resulting in further confusion regarding when processing should require explicit or written consent.

It is the author's belief that health data differs from a simple cold to serious data about illnesses, which means information differs in its degree of risk, as according to Art. 29 (WP), "Health data is the most complex area of sensitive data," (*Article 29 Data Protection Working Party*, 2011, p. 8, 10), and the CJEU in its Bodil Lindqvist decision in C-101/01 adopted a "wide interpretation" for sensitive data where Lindqvist published on her personal internet page personal details about her colleagues, such as their names and work duties, "with reference to one of them who has an injured foot and is on half-time due to medical grounds," (*Bodil Lindqvist*, 2003*,* paras 50, 30, 49, 51) and which constitutes personal data concerning health.

In the author's view, the legislator should consider health data, such as a simple cold, to be protected as personal data, but when personal data discloses an individual's personal data about his/her serious health status, then it should be protected as sensitive data. Sensitive data, including health data, should only be classified as sensitive data based on the potential risk to the individual that may arise from the disclosure of this data.

The author suggests another definition for sensitive data: sensitive data refers to any personal data whose disclosure could reveal information that may pose a risk to the data subject's fundamental rights and freedoms, such as the addresses of judges or victims, and it requires a higher level of protection, such as the previously mentioned closed list of sensitive data in the GDPR and the PDPL.

b) The author's proposed framework for inferences to the PDPL and courts

Although the PDPL has no relevant case law in this area until now, the author frames how Egypt's forthcoming executive regulations and courts should address inferences about sensitive data as follows:

Where processing is based on the data subject's explicit consent

The data subject should be entitled to the right to use his fundamental rights to restrict or limit new inferences outside the specific purpose, such as his/her political opinions, or even to withdraw his consent.

Where processing is lawful regardless of the data subject's consent

When processing is lawful without the data subject's consent in allowed cases according to Art. 2 "… where otherwise permitted by law," and could reveal inferences about sensitive data, the data subject is entitled to use his rights as to object to the processing. Moreover, each of the controller and the processor are obligated to demonstrate the transparency of the logic used in making inferences.

Inferences could be classified as follows:

I. Inferences from personal data that result in revealing sensitive data

Although everyone could purchase the same product of food, it would be for a particular person, identified or identifiable, and when such product is linked to other identification elements, it could reveal sensitive data about his health or financial status. Moreover, inferred data from photos, such as an individual's skin tone or his clothes, could lead to inferences about his religious beliefs (Solove, 2023, pp. 1100, 1123).

II. Inferences from personal data that result in serious risk to the individual

Although addresses are considered personal data, they must be considered sensitive data for particular individuals, such as judges and victims, where revealing such data could result in a serious risk to their privacy (Solove, 2023, p. 1118).

III. Inferences drawn from special data can lead to the revelation of sensitive information

Although personality type or information about personality discloses a person's uniqueness and values, identification of these goals and values, which are not classified as personal or sensitive data, could result in inferences about sensitive data and individuals being classified as religious or political persons (Solove, 2023, p. 1120).

IV. Inferences from collected data or unknown data

Data collected during big data gathering, and the identification of their subjects are impossible, is referred to as collected or unknown data. If the identification

of the data subject becomes possible in any way, either directly or indirectly, those data could result in inferences about sensitive data and must be covered by a high level of protection.

c) The PDPL's Risk Assessment

The risk criterion would face significant enforcement challenges under the PDPL and the Personal Data Protection Center (PDPC), as the law currently lacks a risk assessment mechanism similar to the GDPR's (DPIA), and there is, to date, an absence of relevant case law in this area. Moreover, the PDPC struggles with a weak compliance culture among controllers and processors, combined with ineffective mechanisms for assessing and addressing inferential risks arising from processing. The author suggests the use of analogies and international practices that would guide the legislator and courts in framing an effective risk assessment under the PDPL.

As the data protection officer (DPO) obliges, according to Art. 9 (1), to "… perform a regular evaluation and inspection of the personal data systems and avoid infringement …," which in the author's belief should be of a flexible scope to include a wider assessment in accordance with the processor's obligation, in Art. 5 (8), to "… not to cause any direct or indirect harm to the data subject," which implies assessing risks to individuals' rights, "risk criterion," prior to the processing.

Accordingly, both the processor and the controller must, prior to the processing of personal data, carry out a risk assessment of the impact of that processing to determine whether the processing is likely to lead to inferences that could pose a risk to individuals' rights and freedoms.

3.3 Children's data privacy

Various jurisdictions vary in their protection of children's privacy, including as follows:

A. In the Egyptian PDPL:

The Egyptian PDPL (Arts. 1 and 12) considers child data sensitive in all circumstances, regardless of the child's age, due to their limited awareness of the risks and the consequences of the processing of their data. PDPL requires the legal guardian's consent for processing or disclosing a child's personal data.

Furthermore, Art. 12 provides that when a child participates in a game, competition, or any other activity, the child's data should not be submitted beyond what is necessary for such participation. Accordingly, the author

considers that inferences about the submitted child's data should be considered and protected as sensitive data.

Although the PDPL does not regulate profiling, automated decision-making, educational platforms, or targeted advertising, as the GDPR's Art. 22, the author considers that, in our daily life, these platforms collect data from children at schools or through children's "educational" applications (apps), such as email, IP addresses, etc., and raise significant inferential risks, requiring a high level of protection for inferences about children's data to prevent targeted advertising and profiling.

Profiling may generate sensitive inferences not directly provided by the child or his/her parents, creating inferential risks. Therefore, such processing of children's data or inferences about them should be considered sensitive and protected.

In accordance with the risk criterion, children's data is only protected when the disclosure of it could lead to inferential risks. Nevertheless, the author considers that the PDPL's tendency to protect children's data in all circumstances is more favorable due to children's limited awareness of the consequences of processing their data.

B. In the GDPR and the COPPA:

The GDPR in Art. 8 differentiates between the lawfulness of data processing for children at least 16 years old based on their consent and for children below the age of 16 years old based on their parental or guardian's consent, and that is applied where an 'information society service' is offered directly to the child. However, Art. 8 (1) does not apply where such services are offered by an intermediary (Caglar, 2021, pp. 21-22, 26).

The USA Children's Online Privacy Protection Act (COPPA) (*Children's Online Privacy Protection Rule, COPPA*, 1998) provides parents with control over their children under 13 years old and their data.

While the GDPR's absolute ban provided in Art. 22 does not distinguish between automated decision-making, including profiling concerning adults or children, and does not explicitly prohibit profiling of children, recital 71 provides that automated processing should not apply to children's data, and controllers should not rely on exemptions to justify it. However, WP251 clarifies that this does not present an absolute prohibition (*WP251rev.01*, 2018, p. 19, 28).

Consequently, profiling children's data, particularly in educational platforms, may generate inferences that pose risks to children, and the child's data requires

a high level of protection. Such as Google, which used to collect users' personal data and then target them with advertisements (Krutka et al., 2021, p. 421).

4. Conclusion

Globally, imbalance in global data protection laws is driven by the definitional overlap of personal and sensitive data embedding inferences, as while the Colorado Privacy Act explicitly adopts and recognizes the sensitive nature criterion to protect sensitive data inferences, other jurisdictions such as the aforementioned Indian and Canadian laws do not recognize the terms "sensitive data" or "inferences," which results in a manifested imbalance.

The author attributes that to the lack of personal and sensitive data boundaries and results in an urgent requirement for recognition of the risk criterion instead of the sensitive nature to protect data, which the reveal of could cause serious damage to individuals' rights. This imbalance addresses global lessons for existing and other jurisdictions, which are gathered in:

- Legislators should determine an explicit criterion to distinguish between personal and sensitive data.

- Legislators should explicitly recognize sensitive data and inferences as sensitive data that require a higher level of protection.

- Legislators should provide that "Regarding inferences, the data subject shall have the right to know, review, and access or obtain his/her own inferred data, which is in the possession of any holder, controller, or processor, and shall have the right to correct, edit, and delete his/her deduced data as personal data."

- Data controllers should be required to provide transparency around inferences.

Table 2 Proposed Model for the Egyptian PDPL

Source: The author

Inferred data's criteria	**GDPR's Model (Recitals & Articles & CJEU)**	**Proposed Model Wording for the PDPL & Courts**
Sensitive Nature criterion: • inferences from personal data revealing sensitive data such as health data, religious beliefs, … sexual orientation.	Art. 9, recital 51, and CJEU cases • Case C-394/23. • Case C-252/21. • Case C-446/21. • Case C-184/20. • Case C-21/23.	<u>Definitional boundary</u> • Personal data means any information that relates to an identified or identifiable natural person, such as name … etc • Sensitive data refers to any personal data whose disclosure could reveal of information that may pose a risk to the data subject's fundamental rights and freedoms, such as the addresses of judges or victims, and it requires a higher level of protection. <u>Consent:</u> Processing of inferred data shall be subject to the data subject's explicit written consent where such data reveals risk to the data subject's rights. <u>Transparency:</u> Each of the processor and the controller is required to comply with transparency obligations. <u>Data subject's rights with inferences:</u>

		The data subject is entitled to the right to access, correct, and delete his/her inferred data.
Risk criterion: inferences that reveal information the disclosure of which may result in significant harm, risk, or discrimination for individual's rights and freedoms	• Case C- 667/21. • Case C- 136/17.	<u>Enforcement challenges regarding Risk Assessment:</u> The PDPC is the authorized authority to issue licenses for data processing but lacks a risk assessment mechanism. • *Suggested solutions:* The data protection officer (DPO) obliges to perform a regular evaluation and inspection of the personal data. Each of the processor and the controller shall, prior to the processing of personal data, carry out a risk assessment of the impact of that processing to determine whether the processing is likely to result in a risk to the individuals' rights and freedoms.

Bibliography
Journal Articles

Ali, R. M. (2025). Sensitive Digital Financial Data in Transactions of Electronic Commerce in accordance with Law No. 151 of 2020. *Legal Journal, Faculty of Law (Al Khartoum Branch), Cairo University*, *23* (7), 4063–4142. https://doi.org/10.21608/jlaw.2025.356524.1151

Caglar, C. (2021). Children's right to privacy and data protection: Does the article on conditions applicable to child's consent under the GDPR tackle the challenges of the digital era or create further confusion? *European Journal of Law and Technology, 12*(2). https://ejlt.org/index.php/ejlt/article/view/828/1025

Citron, D. K., & Solove, D. J. (2021). Privacy Harms. *SSRN Electronic Journal*. 793–863. https://doi.org/10.2139/ssrn.3782222

Eldomiaty, T. M. (2022). Digital Consent to the processing of Personal Data: A Comparative Study. *Journal of Law and Emerging Technology*, *2*(1), 13–138. https://doi.org/10.54873/jolets.v2i1.60

Gupta, I., Philip, S. S., & Naithani, P. (2024). Introduction to EU Data Protection Law. In I. Gupta, S. S. Philip, & P. Naithani, *Introduction to Data Protection Law*, 1–58. Springer Nature Singapore. https://doi.org/10.1007/978-981-97-6355-9_1

Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*, *28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Jain, P., Gyanchandani, M., & Khare, N. (2016). Big data privacy: A technological perspective and review. *Journal of Big Data*, *3*(1), 25. https://doi.org/10.1186/s40537-016-0059-y

Kohli, S. (2023). *Data Protection in light of the Digital Personal Data Protection Act 2023*. ResearchGate. https://www.researchgate.net/publication/393353824_DATA_PROTECTION_IN_LIGHT_OF_THE_DIGITAL_PERSONAL_DATA_PROTECTION_ACT_2023

Kovalenko, Y. (2022). The Right to Privacy and Protection of Personal Data: Emerging Trends and Implications for Development in Jurisprudence of European Court of Human Rights. *Masaryk University Journal of Law and Technology*, *16*(1), 37–58. https://doi.org/10.5817/MUJLT2022-1-2

Krutka, D. G., Smits, R. M., & Willhelm, T. A. (2021). Don't Be Evil: Should We Use Google in Schools? *TechTrends, 65(4),* 421–431. https://doi.org/10.1007/s11528-021-00599-4

Kumar, Y., Marchena, J., Awlla, A. H., Li, J. J., & Abdalla, H. B. (2024). The AI-Powered Evolution of Big Data. *Applied Sciences*, *14*(22), 10176. https://doi.org/10.3390/app142210176

Mahdy, A. M. (2025). Acceptance of Digital Processing of Personal Data. *Legal Journal, Faculty of Law (Al Khartoum Branch), Cairo University*, *23*(7), 4247–4474. https://doi.org/10.21608/jlaw.2025.360953.1181

Mahmoud, S. A., (2024). Protection of Digital Personal Data in accordance with Egyptian Personal Data Protection Law No. 151 of 2020. *Journal of Legal and Economic Sciences, Faculty of Law, Ain Shams University*, *66*(1), 1439–1482. https://doi.org/10.21608/jelc.2024.341026

Mesarčík, M. (2020). Apply or not to apply?: A. *Bratislava Law Review*, *4*(2), 81–94. https://doi.org/10.46282/blr.2020.4.2.171

Nguyen, N. S., Tran, B. T., Le, T. N. L., & Nguyen, N. Q. (2025). The impact of digital environmental, social, and corporate governance on consumer purchase intention. *Journal of Governance and Regulation*, *14*(2), 18–27. https://doi.org/10.22495/jgrv14i2art2

Quinn, P., & Malgieri, G. (2020). The Difficulty of Defining Sensitive Data – the Concept of Sensitive Data in the EU Data Protection Framework. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3713134

Rashad, S. S. (2024). Strengthening the legal protection of sensitive personal data in the fields of inferences: A comparative study. *Journal of Economic and Legal Studies, Faculty of Law, Mansura University*, *14*(88.), 1043–1319. https://doi.org/10.21608/mjle.2024.363494

Rupp, V., & Von Grafenstein, M. (2024). Clarifying "personal data" and the role of anonymisation in data protection law: Including and excluding data from the scope of the GDPR (more clearly) through refining the concept of data protection. *Computer Law & Security Review*, *52*, 105932–105957. https://doi.org/10.1016/j.clsr.2023.105932

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Solove, D. J. (2022). The Limitations of Privacy Rights. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4024790

Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *SSRN Electronic Journal*, 1081–1138 https://doi.org/10.2139/ssrn.4322198

Solove, D. J., & Schwartz, P. M. (2019). ALI Data Privacy: Overview and Black Letter Text. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3457563

Soria-Comas, J., & Domingo-Ferrer, J. (2016). Big Data Privacy: Challenges to Privacy Principles and Models. *Data Science and Engineering*, *1*(1), 21–28. https://doi.org/10.1007/s41019-015-0001-x

Staunton, C., Edgcumbe, A., Abdulrauf, L., Gooden, A., Ogendi, P., & Thaldar, D. (2025). Cross-border data sharing for research in Africa: An analysis of the data protection and research ethics requirements in 12 jurisdictions. *Journal of Law and the Biosciences*, *12*(1), lsaf002. https://doi.org/10.1093/jlb/lsaf002

Turnšek, E., & Kraljić, S. (2024). The protection of sensitive personal data and privacy in the us and eu with a focus on health data circulating through health apps. *Balkan Social Science Review*, *24* (24), 179–205. https://doi.org/10.46763/BSSR242424179t

Voss, W. G. (2021). The CCPA and the GDPR Are Not the Same: Why You Should Understand Both. *CPI Antitrust Chronicle*, *1*(1), 7–12. https://ssrn.com/abstract=3769825

Wanjale, K., Mangla, M., & Marathe, P. (2021). Security of Sensitive Data in Cloud Computing. In S. N. Mohanty, J. M. Chatterjee, M. Mangla, S. Satpathy, & S. Potluri (Eds.), *Machine Learning Approach for Cloud Data Analytics in IoT*, 1st ed., 99–118. Wiley. https://doi.org/10.1002/9781119785873.ch5

Widjaja, G. (2024). Balancing Between Fiscal Interests and Privacy Data Protection. *Contemporary Readings in Law and Social Justice*, *16*(1), 787–794. https://crlsj.com/index.php/journal/article/view/183/77

Wiedemann, K. (2020). The ECJ's Decision in "Planet49" (Case C-673/17): A Cookie Monster or Much Ado About Nothing? *IIC - International Review of Intellectual Property and Competition Law*, *51*(4), 543–553. https://doi.org/10.1007/s40319-020-00927-w

Acts and Regulations

Article 29 Data Protection Working Party. (2018, February 6). *Guidelines on Automated individual decision-making and profiling for the purposes of*

Regulation 2016/679. European Data Protection Board. https://ec.europa.eu.newsroom/article29/items/612053/en

California Consumer Privacy Act (CCPA) of 2018, Cal. Civ. Code § §§ 1798.100–1798.199 (2018). https://cppa.ca.gov/regulations/pdf/ccpa_statute.pdf

California Privacy Protection Agency. (2020). *California Privacy Rights Act*, *(CPRA)*. https://thecpra.org/

Colorado Privacy Act Rules. (2023). Colorado Department of Law. https://www.sos.state.co.us/CCR/GenerateRulePdf.do?ruleVersionId=10872&fileName=4%20CCR%20904-3

Data (Use and Access) Act. (2025). Uk Government. https://www.legislation.gov.uk/ukpga/2025/18/pdfs/ukpga_20250018_en.pdf?utm_source

Digital Charter Implementation Act. (2020). Office of the Privacy Commissioner of Canada. https://www.sfu.ca/~palys/BillC11-PrivacyCommissionerResponse.pdf

Digital Charter Implementation Act. (2022). Canadian Parliament. https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading

Digital Personal Data Protection Act. (2023). Ministry of Electronics and Information Technology. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, European Parliament. (1995). https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng

Egyptian Civil Law No. 131 of 1948. (1948), Official Gazette. https://brill.com/display/book/9789004479906/back-11.xml

Egyptian Personal Data Protection Law No. 151 of 2020, issue No. 28 (bis) E. (2020, July 15), Official Gazette. https://www.privacylaws.com/media/3263/egypt-data-protection-law-151-of-2020.pdf

European Commission*, Article 29 Data Protection Working Party, Advice Paper on Special Categories of Data ("Sensitive Data")*, (2011), European Commission. https://ec.europa.eu/justice/article-29/documentation/other-

document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf

European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679*, (2020).https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

Federal Trade Commission. (1998). *Children's Online Privacy Protection Rule, (16 C.F.R. part 312)*. Electronic Code of Federal Regulations. https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). http://data.europa.eu/eli/reg/2016/679/oj

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). (2023). https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). (2024). http://data.europa.eu/eli/reg/2024/1689/oj

UAE Federal Decree No. (45) of 2021 Concerning the Protection of Personal Data, Official Gazette. https://www.uaelegislation.gov.ae/en/legislations/1972/download

UK Government. (2018). *Data Protection Act*. Uk Government. https://www.legislation.gov.uk/ukpga/2018/12/enacted

UK. (2024a). *Special category data*. Information Commissioner's Office. https://cy.ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/special-category-data/

UK. (2024b). *Special category data*. Information Commissioner's Office. https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-for-the-use-of-personal-data-in-political-campaigning-1/special-category-data/?utm_source

UK. (2024c). *What is special category data?* Information Commissioner's Office. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/?utm_source

Court Decisions

Agentsia Po Vpisvaniyata v Ol, ECLI:EU:C:2024:805 ___ (Court of Justice of the European Union 2024). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62023CJ0200

Bodil Lindqvist, ECLI:EU:C:2003:596 ___ (Court of Justice of the European Union 2003). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62001CJ0101

GC and Others v Commission Nationale de l'informatique et Des Libertés, ECLI:EU:C:2019:773 ___ (Court of Justice of the European Union 2019). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62017CJ0136

Maximilian Schrems v Meta Platforms Ireland Ltd, ECLI:EU:C:2024:834 ___ (Court of Justice of the European Union 2024). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0446

Medizinischer Dienst Der Krankenversicherung Nordrhein, ECLI:EU:C:2023:433 ___ (Court of Justice of the European Union 2023). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CC0667

Meta Platforms and Others (General Terms of Use of a Social Network), ECLI:EU:C:2023:537 ___ (Court of Justice of the European Union 2023). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0252

Mousse v Commission Nationale de l'informatique et Des Libertés (CNIL) and SNCF Connect, ECLI:EU:C:2025:2 ___ (Court of Justice of the European Union 2025). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62023CJ0394

ND v DR, ECLI:EU:C:2024:846 ___ (Court of Justice of the European Union 2024). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62023CJ0021

OT v Vyriausioji Tarnybinės Etikos Komisija (Lithuania), ECLI:EU:C:2022:601 ___ (Court of Justice of the European Union

2022). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62020CJ0184

Patrick Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779 ___ (Court of Justice of the European Union 2016). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0582