March 15, 2021
2 Nissan, 5781

Data minimization[1]

Background

The digital age is characterized by the collection and storage of extensive data, including personal data, in databases. The data is stored and processed for different and diverse purposes. The collection of data and its storage are considered necessary processes in the digital day-to-day reality.

Nevertheless, in many cases the data collected and stored is in fact unnecessary or non-relevant for the purpose it was initially collected for, or for the purposes of the database in which it is stored (hereinafter 'excess data'). Data can become excess data already in the initial stage of the its collection, and can also become such during its storage over time.

The collection and storage of excess data increase the risk to privacy. As explained in the examples below, the collection of excess data beyond necessary constitutes, in and of itself, an infringement of privacy. In addition, data stored in databases can leak, be exposed in the public domain, or be used by unauthorized parties. Therefore, the collection and storage of excess data unnecessary for the purpose for which it was collected or for the purpose of the database in which it is stored, puts privacy at risk. The minimization of the excess data can therefore minimize the infringement of privacy that might be caused as a result of data collection and its leak. In addition, as explained hereinafter, data minimization can also correspond with the interests of those who collect and store data.

In this document the Privacy Protection Authority (hereinafter: the 'PPA') will review the requirements laid down in the law, extrapolate from these requirements the principle of data minimization and present additional recommendations for the minimization of collection and storage of excess data in databases. This document is published for public hearing. The PPA will conduct an examination of the regulatory effects of this document, *inter alia*, in light of the comments received from the public.

[1] The document reviews the provisions of the law and presents the interpretation and recommendations of the Privacy Protection Authority regarding data minimization.

The principles of privacy protection laws in a nutshell

The right to privacy is a constitutional right that stems from the concept of human dignity, and a civil right that reflects the basic right of an individual "to be let alone." Privacy, for the purpose of this matter, is consistent with the need of people to stay anonymous, and to be protected from inappropriate intervention of the State authorities and from other entities in their lives. This approach is manifested in the Israeli law, *inter alia*, in the provisions of Article 2(1) of the Privacy Protection Law, 5741-1981 (hereinafter: the ''Privacy Protection Law' or 'the Law') which stipulates one of the definitions of "privacy infringement" as "Spying on or trailing a person in a manner likely to harass him."

The Israeli privacy protection laws, that are primarily regulated under the Basic Law: Human Dignity and Liberty, the Privacy Protection Law and the regulations promulgated thereunder, permit the collection and the processing of data about a person only on the condition that the law permits such actions, or based on the consent of the data subject. Therefore, **the principle of consent** constitutes one of the main key principles enshrined in the Israeli Privacy Protection Law. This principle reflects the control of an individual over data related to him. This principle is manifested, *inter alia*, in Article 1 of the Privacy Protection Law, which states that, "No person shall infringe the privacy of another without his consent." According to the Law, consent for the purpose of this matter should be 'informed' i.e., consent that is granted only after a person understands the meaning of his consent, and its ramifications.

The proper application of this principle mandates the recipient of the consent to inform the individual granting the consent the entire material information that is relevant for making the decision and granting the consent. The party seeking consent must specify, *inter alia*, which data will be collected after obtaining the consent, what uses will be made with the data, to whom the data might be transferred and for what purpose. The explanation should be clear, direct and made in a clear and accessible language, and should include further information regarding the rights of the data subject.

Another key principle in the Privacy Protection Law is the **purpose limitation principle**. According to this principle, regulated under Articles 2(9) and 8(b) of the Privacy Protection Law, the use of data can be made only for the purpose for which the data was collected or initially provided. In this sense, the use of data for a purpose other than the purpose for

which it was collected, and without obtaining the data subject's consent constitutes an infringement of privacy that can amount to a criminal offence which can lead up to 5 years of imprisonment. The disclosure of data by an employee, database owner (controller) or possessor, not for the purpose of his task, might also be considered as a criminal offense pursuant to the provisions of article 16 of the Law. The Privacy Protection Law and the regulations promulgated thereunder also lay down different obligations with regard to database registration and data security including, *inter alia*, the obligation to consider the continuation of data storage as depending on the purpose of its collection.

The Privacy Protection Law also refers to the **rights of the data subject**. Thus, pursuant to Article 11 of the Law, a request for personal data with a view to the keeping and use thereof in a database shall be accompanied by a notice, indicating whether that person is under a legal duty to deliver that data or whether its delivery depends on his consent. Article 13 of the Law grants to the data subject the right to access the data related to him and Article 14 of the Law entitles the data subject to demand its correction, under the proper circumstances.

Same as any other rights, the right to privacy is not absolute, and there could definitely be circumstances in which other interests will justify a certain compromise of this right, to the extent that the law recognized such circumstances. This approach is reflected, *inter alia*, in Article 18 of the Privacy Protection Law that lays down a list of defenses that a defendant in a civil or a criminal trial is entitled to invoke against an argument regarding infringement of privacy in accordance with the Law. In any case, such infringement of privacy, even when it is permitted, should be committed in accordance with the purpose of the provisions of the law and according to the general principles of reasonableness and good faith, and the demand for proportionality, where relevant.

Excess data and the risks to privacy

This part provides a definition of the data minimization principle and will elaborate on the risks to privacy that might be caused as a result of data collection and storage in databases.

Excess data – definition and legal source

This part defines excess data and will refer to the legal sources of such a definition. The different arrangements set out in the law that refer, both directly and indirectly, to data minimization, will be elaborated further below in this document.

Article 2(9) of the Privacy Protection Law states that the use of data regarding the private affairs of a person or its delivery to another without consent and not for the purpose for which it was provided, constitutes an infringement of privacy. In addition, Article 8(b) of the Law states that the data stored in a database may not be used, but solely for the purpose for which the database was created[2]. Article 2(A)(2) of the Privacy Protection Regulations (Data Security) 5777-2017 (hereinafter: the 'Regulations' or the 'Data Security Regulations') states that the database owner (controller) is required to draw up a database definitions document on which he will state, *inter alia*, the description of the purposes of use of data in the database[3]. Article 2(c) of the Regulations states that, "The database owner will review annually whether the data stored in the database exceeds what is required for the database purposes."

In light of the above it transpires that excess data is data about a person that includes data items which are irrelevant and unnecessary for accomplishing the purpose for which the data was initially collected, or for accomplishing the objects of the database in which it is stored, or data that is no longer required for these purposes.

[2] Data is defined in chapter B of the Privacy Protection Law as "data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person."

[3] Section 9(b)(2) of the Privacy Protection Law states that the purposes for which the database was established and the purposes for which the data is intended, should be stated also in an application for database registration. These purposes may be viewed by the public by virtue of the provisions of section 12 of the Law.

Therefore, excess data can be created already during the initial collection stage, or during the stage of its transfer between different entities[4], or become such also during the period of its storage over time in the database. In the last scenario, data that was relevant and compatible to the purpose for which it was collected and for the purpose of the database in which it is stored, became excess during the time of its storage in the database, in light of a change in circumstances such as accomplishment of the original purpose, collection of additional data and the like.

Data can be considered as excess data, *inter alia*, in light of its scope, type, the duration of its storage etc. In this sense, data can be considered as excess data in circumstances in which the type of the data that was collected or the period of time of its storage are not necessary for the purpose of the collection or the purpose of the database in which it is stored.

For example, part of the data regarding customers stored by a communication company for the purpose of marketing products for its customers and improving the terms of service, might become excess data when customers cancel their subscription and switch to competing company. Another example might be a company leasing off-road bikes that photocopies the driver's licenses of its customers before they take an off-road trip, in addition to a document in which they declare that they hold a proper driver's license. After the trip is completed, and assuming there were no special events, it seems that there is no longer any need to store a copy of the driver's license and such data became excess data, especially in light of the fact that a driver's license includes sensitive data regarding its owner such as their age and residential address. Another example, that was discussed in an Israeli court, is that of an insurance company which received from the Execution Office a foreclosure writ due to its status as a holder of the assets of a debtor, for the purpose of seizing money that belongs to that debtor, but continues to retain the data included in the foreclosure writ even after the relevant legal proceeding was completed. In this matter the Supreme Court stated that 'no use of data that reached an entity such as an insurance company or a bank on a certain matter should be used for any requirement outside the scope

[4] Section 23E of the Privacy Protection Law that deals with data transfer between public bodies refers to excess data as 'other data' stored in a the same file with data that may be transferred between public bodies pursuant to the provisions of sections 23B or 23C of the Law.

of the original permitted use, and this data **should be removed from the institutional memory of these entities for any purpose, except for the original purpose**."[5]

In other words, the criterion which determines whether data is excess or necessary for the purposes of the database is not just a quantitative criterion that concerns the scope of the data, but a criterion that examines the entire aspects of the data and its relevancy to the purposes of the collection and the database.

In light of the foregoing, we can conceptualize the principle of minimization of excess data as a principle according to which it is necessary to avoid, to the extent possible, the collection and the storage of data about a person that is not necessary for the purpose of the collection or for the purpose of the database in which it is stored. According to this approach, it is necessary to collect and store only the minimum data required and essential for the said purposes, in terms of the scope of the data that is stored, the type of the data, the duration in which the data is stored and the like.

The collection of excess data, the use of data about the private affairs of a person (including the mere storage of the data) when the said data is not required for the purpose for which it is provided or for the purpose of the database, or the continuation of use of the said data or information, are in violation of the purpose limitation principle set out in Articles 2(9) and 8(b) of the Law, and create unnecessary data security risks. Therefore, they constitute an infringement of privacy and breach the provisions of the Privacy Protection Law[6].

[5] AdminA 7043/12 *I.D.I. Insurance Co. Ltd. v. Ministry of Justice – Israeli Law, Information and Technology Authority (ILITA) – Database Registrar* (published in Nevo, 15.1.14). See also the comprehensive judgment given by the District Court, which was the subject of the abovementioned appeal to the Supreme Court (AP AdminC 24867-02-11 *I.D.I. Insurance Co. Ltd. v. Ministry of Justice – Israeli Law, Information and Technology Authority (ILITA) – Database Registrar* (published in Nevo, 1.8.12)). In this case, based on the data contained in the writ of foreclosure that it stored, the insurance company refused the request of a debtor to purchase insurance. The District Court stated that data concerning the existence of a writ of foreclosure on the assets of a person is private protected data, and that insurance companies and financial entities are not entitled to use this data for purposes exceeding the scope of the original writ of foreclosure, such as the classification of existing or potential customers. The Supreme Court sided with the judgment given by the District Court, along with its reasoning.

[6] See, for example PPA Directive no. 4/2012 "The use of security and surveillance cameras and the databases of the photos captured in them":
https://www.gov.il/BlobFolder/policy/surveillance_cameras_guidelines/he/The%20use%20of%20security%20cameras.pdf.

Excess data – the risks to privacy

In the digital reality we live in, extensive data on individuals that is collected and stored in databases owned by private companies and public authorities, is in fact excess data. We could say that the collection and the storage of excess data – that is not necessary and that is not relevant for the purpose of the collection or the database – are customary practices among many data companies and corporations[7]. These circumstances could constitute an infringement and risk to privacy, in three different major realms:

A. Infringement of privacy caused as a result of the collection and use of excess data that is not required for the purpose of accomplishing the goal for which the consent was granted

As already noted above, the collection and use of data not for the purpose for which the consent to collect and use was granted is prohibited and constitutes an infringement of privacy[8]. This reflects violation of the principles of consent and the purpose limitation principle that were presented earlier. In a deeper sense, this violation also reflects breach of autonomy of the individual and affects his ability to make decisions regarding his life and the data relating to him.

This violation will be even worse in circumstances in which the collection and the use of the data were performed not by virtue of consent (however in light of an obligation set out in the law) or in circumstances in which the consent was granted within the framework of unequal powers between the party granting the consent and its recipient. In general, in such circumstances the need to adhere to the purpose limitation principle is further stressed, i.e., that the data that will be collected will

[7] A famous quote that was made for the purpose of this matter is that of Jeff Bezos, CEO of Amazon Company who said that: "We never throw away data." For a response to this statement see: https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/?sh=54aba8751da4. Prof. Shoshanna Zuboff argues for the purpose of this matter that data corporations will never only settle for the data for the purpose for which this data is initially collected, and these corporations have a kind of an inherent interest to collect excess behavioral data (behavioral surplus). For the purpose of this matter see: Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INF. TECHNOL. 75 (2015); Shoshana Zuboff, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

[8] Regarding the imposition of limitations on the collection of data as an integral part of the right to privacy see HCJ 6732/20 ***Association for Civil Rights in Israel v. The Knesset*** (published in Nevo, 1.3.21) para. 12 in Justice Barak-Erez's opinion.

be only data that is required for accomplishing the purpose of the collection or the database purpose[9].

B. Risk to infringement of privacy as a result of the storage of excess data

The mere storage of excess data that is not relevant or necessary for the purpose of the database constitutes a risk to privacy. This risk stems, *inter alia*, from the concern that the storage of excess data might open the way to additional purposes and uses of the data, including the processing of such data, its cross-referencing with other data and its transfer to others. The storage of excess data might therefore, result in breach of the purpose limitation principle, hence it constitutes a risk to privacy infringement.

C. Risk to infringement of privacy as a result of the leak and disclosure of excess data

In general databases are not immune from data breach. The data stored in them might leak, be exposed to the public, and hence can be subject to the use of unauthorized entities. Data leak can be caused as a result of a failure by the possessor (processor), by the owner of the database (controller), or as a result of a deliberate hack, even if proper security measures were taken. The unnecessary storage of data therefore creates an unnecessary security risk and might also constitute a violation of the duty of security set out in Article 17 of the Law and in the Data Security Regulations. In the current digital reality, the ability to cross-reference data and to distribute it is greater than ever and gradually increases over time. In this sense, data that was exposed can no longer be removed or deleted, and hence, ordinarily, **the harm caused as a result of such exposure is irreversible**. In such circumstances, the greater the data that is stored is – the greater the risk to infringement of privacy that will be caused as a result of the leak and the exposure of the data becomes[10].

[9] Indeed, chapter D of the Privacy Protection Law permits, under the conditions stated therein, to transfer data between public bodies, even if such transfer is made for a purpose that deviates from the original purpose of the collection that was permitted to the transferring body – however while laying down detailed conditions for the minimization of collection of excess data as stated in section 23E of the Law, as also stated further below in this document.

[10] On the creation of an increased risk for data leak as an expression of an additional dimension of the right to privacy see the judgment given in the **Association for Civil Rights in Israel**, footnote 8, *supra*, para. 14 in Justice Barak-Erez's opinion.

One example for the purpose of this matter is the phenomenon of ransomware. Ransomware is a malware in which attackers penetrate databases, steal the data stored in them and threaten that if they do not receive payment, they will expose the data in the public domain, thereby infringing the privacy of the people who are subjects of the data and the reputation of the company from which the data was stolen. Another example that emphasizes the risk to privacy as a result of a leak of excess data is related to social engineering activity after a data breach event. When excess data leaks it is reasonable to assume that the data subject is not aware of such a leak, for the simple reason he assumes that this data was not collected to begin with, or that it was not stored over time. In view of these circumstances, in which the data subject is not aware that certain data related to him has leaked, his ability to mitigate his damage, for example by changing the data or hedging his risks, is impaired.

In conclusion, **the collection and storage of excess data that is not necessary for the purpose it was initially collected or for the purpose of the database, and the use of such data, violate the right to privacy and jeopardize it. The minimization of excess data – both during the stage of initial collection and during the period in which such data is stored in the database – can minimize and diminish the risks to infringement of privacy**.

Minimization of excess data in the provisions of the law

So far, we defined excess data, the reasons why the storage or collection of such data might amount to infringement of privacy, and the risks to privacy that stem from the collection, storage and use of excess data. This part will specify the provisions of the law that refer to data minimization in the context of Israeli privacy law.

Israeli privacy laws lay down a duty to minimize data. As already noted, Article 2(9) of the Privacy Protection Law states that the using, or passing on to another, data on a person's private affairs otherwise than for the purpose for which it was given constitutes an infringement of privacy. This article lays down an obligation to collect and store data, from the start, solely for the purpose for which the consent for its collection was granted, and when the collection was performed by virtue of a statute – for the purpose set out by the

statute. **This article in fact stipulates that the collected data must be relevant and related to the purpose of its collection, and therefore expresses the duty of minimization of excess data during the initial stage of the data collection**.

Since the term 'use' is interpreted as also including the storage of data, Article 2(9) of the Law in fact lays down the duty to minimize data both during the stage of data collection and during the stage of data storage. In the Isakov Case the National Labor Court held in this matter that "According to the purpose limitation principle, the initial purpose of data collection should be regarded as linked to the data that was collected in all its transformations. Therefore, the employer cannot use data that exceeds the initial purpose for which it was collected."[11]

The issue of data minimization during the stage of data storage can also be found in Article 8(b) of the Privacy Protection Law which states that, "A person shall not use data in a database that requires registration under this article except for the purpose for which the database was established." Article 2(c) of the Data Security Regulations states that a database owner (controller) will review, once a year, whether the data that he stores in the database exceeds what is required for the database purposes.

Article 2(c) of the Regulations actually expresses the gap that might exist between data that is stored in a database and required for its purpose, and excess data that is not required for such purpose. **From this article one can learn that failure to minimize excess data by a database owner (controller), in circumstances in which he himself reached a conclusion that the data stored in his database is in fact excess data, might constitute a violation of the Data Security Regulations and infringement of privacy**.

The duty to minimize excess data is also set out expressly in Article 6 of the Privacy Protection Regulations (Terms of Holding Data and Its Maintenance and Procedures for Transfer of Data between Public Entities) 5746-1986 (hereinafter: the 'Data Transfer between Public Entities Regulations') which states that a public entity that receives data in accordance to the said Regulations "Will, upon the receipt of such data, separate immediately the excess data and will delete it immediately."

[11] LabA (National) 90/08 ***Tali Isakov Inbar v. The State of Israel – Supervisor of Women's Labor et al.***, 38 (published in Nevo, 8.2.2011). For the avoidance of doubt, it is clarified that the purpose limitation principle is expressed directly in section 2(9) of the Protection of Privacy Law.

These Regulations were promulgated further to the provisions of Article 23E(b) of the Privacy Protection Law which states that the transfer of excess data between public entities in accordance with the provisions of Article 23E(a) may only be imparted "if procedures have been prescribed preventing any use being made thereof" ."[12]

So far, we provided a general, direct and basic reference to the issue of data minimization. As stated further below, the Israeli privacy protection laws also address indirectly the issue of excess data, in specific contexts relating to the storage and transfer of data.

Such a reference can be found in Article 14 of the Privacy Protection Law which concerns the correction of data following a data subject's request. This article states that, "a person who, on inspecting any data about himself, and finds that it is not correct, not complete, not clear or not up to date, may request the database owner or, if such owner is a non-resident, the database possessor, to amend or delete the data." **The right of the data subject to demand the correction of data relating to him on the ground that the data is not updated, means that in certain circumstances non-updated data about a person might also be considered as excess data, and that person is entitled to request its correction or deletion**.

Another indirect source supporting the existence of the principle of data minimization in Israeli law can be found in Article 1(3) of the Privacy Protection Regulations (Transfer of Data Abroad) 5761-2001 (hereinafter: the 'Transfer of Data Abroad Regulations'). This article stipulates that data stored in databases in Israel will not be transferred to databases abroad unless the law of the destination state provides a data protection level which does not fall below the data protection level set out in Israeli law, *mutatis mutandis*, and lays down principles, including the principle that the "data gathered shall be accurate and updated."

An example for the importance of minimizing excess data as part of the minimization of the infringement of privacy, and the specific duty stemming therefrom can also be found in Israeli courts rulings. In LabA (National) 40711-04-17 *Fisher Pharmaceutical Industries Ltd. v. Avraham Shtater* (published in Nevo, 4.3.18) the National Labor Court stated that an employee's tracking data would be delivered to the employee before being

[12] This arrangement is laid down in the provisions of chapter D of the Privacy Protection Law which enables, in certain circumstances, the transfer of data between public bodies, not based on the consent of the data subject and not according to the purpose limitation principle.

forwarded to the employer, for the purpose of enabling employees to redact excess data that is irrelevant for the purpose of reviewing the manner of their conduct during work hours. The Court stated that: "**The omission of excess data enables the partial discovery of data where the general and broad disclosure causes disproportionate harm to legal interests that are worthy of protection, including the right to privacy…the manner of transferring this data contributes to the minimization of the infringement of privacy**" (emphasis not at source). The judgment is an example of circumstances in which the duty to minimize data might be imposed in different contexts and in different points in time, in order to minimize the infringement of privacy.

Another example in this matter is the judgment that was given in the I.D.I case, that was mentioned earlier. In its judgment the Supreme Court held that a PPA guideline - stipulating that a third-party holding the rights of a debtor is not entitled to store data contained in a foreclosure writ it received from the Excecution Office, and cannot use the data for the purpose of classifying customers - is in accordance with the provisions of the law.

The PPA's interpretation regarding the scope of the data minimization principle is also manifested in specific contexts, such as the PPA guideline regarding the use of surveillance cameras[13]. This guideline refers to data minimization, both during the stage of data collection, and during the stage of its storage in databases.

Article 3.1.2.1 of PPA Guideline No. 4/2012 [The PPA's guidelines on the use of surveillance cameras in the public space, published in 2012] states that a camera should be installed in a way that its place and angle only cover the relevant areas, with minimal coverage of the area irrelevant for the purpose of placing the camera. Article 3.1.2.2 of the guideline states that the minimal number of cameras that is essential for accomplishing their purpose should preferably be installed, since more cameras than necessary might cause the collection of excess data, thus infringing the privacy of the people filmed by them. This guideline, by its very own nature, is intended to minimize, from the start, the data that can be collected by use of the cameras. Article 3.1.4.1 of the guideline states expressly that 'the storage of photos, after such photos are no longer needed, constitutes a violation of the purpose limitation principle and creates unnecessary data security risks, and therefore also infringes the constitutional right to privacy in a disproportional manner."

[13] See the link to the Directive, footnote 6, *supra*.

This guideline purports to minimize the data stored in databases of surveillance cameras, which became excess data after its collection.

So far, we have elaborated on data minimization in Israeli privacy laws[14]. As already noted, some of the legal provisions might, in certain circumstances, oblige the party collecting the data, the database owner (controller) or possessor (processor) to minimize excess data.

Notwithstanding the above, there could be specific and extraordinary circumstances in which the database owner (controller) or possessor (processor) will be able to store data that could have been considered as excess data with relation to the major, initial purpose of its collection, when the storage of the data (or parts thereof) is essential for implementing the initial purpose, for example when it is necessary for future litigation or by virtue of a statutory duty[15]. In these circumstances, the data will not be considered excess data, within its meaning in this document.

Minimization of excess data as an interest of entities collecting and storing data

As explained hereinafter, the application of the data minimization principle, both in the stage of data collection and during its storage, might correspond with the interests of entities that collect and store personal data.

Reduction of economic inputs – compliance with the law provisions concerning data protection requires investment of extensive inputs. Thus, for example, in accordance with the provisions of the Israeli law, the more extensive or the more sensitive the scope of the

[14] The issue of data minimization is regulated expressly in EU law in the General Data Protection Regulation (GDPR). Article 5(1)(c) of the GDPR states that personal data should be: "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization')." The meaning of this article is that personal data collected and stored in a database should be satisfactory for attaining the purpose of the database, relevant and related to this purpose, and not deviate from the scope of action required for attaining this purpose. In accordance with the provisions in this article, and based on the accountability principle provided for in the GDPR, entities who collect and store personal data, and are subject to the GDPR, should be able to prove that they apply proper measures for the purpose of assuring that this data is necessary for attaining the goals, i.e., that they do not collect or store excess data.

[15] See, for example the definition of the limitation period in the Statute of limitations, 5718-1958. As for statutory duties to store data see, for example, the Archive Regulations (Eradication of Archive Materials in State Institutions and Municipalities), 5746-1986.

data stored in the databases, the higher the level of data security required[16]. In this sense, **data minimization that will naturally result in the minimization of the scope and types of data stored in databases, might also result in reduction of the costs and investment required for the purpose of protecting this data**. This point is especially critical with relation to the entities which are subject to the GDPR as a result of their commercial operations, and are required to make investments for the purpose of complying with the principle of accountability and show that the data that they collect and store is indeed relevant and necessary according to the GDPR. The integration of the data minimization principle might assist those entities and result in reduction of costs.

Reduction of the infringement of privacy from a public aspect and its financial implications – The collection and storage of excess data increase the risk of infringement of privacy. This infringement, for example as a result of data leak and its exposure in the public domain, might expose the corporation in charge of the data protection to lawsuits. Such an exposure might also harm the reputation of the corporation. Therefore, **since the minimization of excess data might also result in the minimization of the degree of privacy infringement that will be caused as a result of the data leak –corporations have an interest to reduce the data they store, to the extent possible**.

Reduction of the regulatory burden – as aforementioned, the provisions of the law might, in certain cases, compel the database owners (controllers) and possessors (processors) to minimize the data they store. Thus, for example, pursuant to the provisions of Article 14 of the Privacy Protection Law, a database owner (controller) can be requested by a data subject to delete data about him, if it is not accurate. Therefore, **in the event corporations apply the approach of minimization of excess data, while performing real and absolute deletion of the said data, this might relieve the statutory and regulatory burden imposed on them**. As already noted, this aspect is especially relevant to corporations that are required to act in accordance with the principle of accountability set out in the GDPR.

[16] The Data Security Regulations lay down three data security levels that apply to the databases – low, medium and high. These levels differ based on several features, including the sensitivity and the scope of the data. See Article 1 of the Regulations as well as the first and second schedule thereto.

Strengthening public trust – the lack of trust and the fear from data leaks lead to circumstances in which considerable parts of the public avoid using certain online media or provide deliberately incorrect or inaccurate data about themselves, while using such media. The commitment of corporations to comply with the data minimization principle, together with their compliance with the provisions of the law in terms of data security, might result in the strengthening users' trust, with all that goes with it.

Data minimization – the legal requirements and the Privacy Protection Authority recommendations

A. It is recommended that entities collecting data based on consent or by virtue of a statute, assure that the data they collect is relevant, necessary and required for the collection and database purposes. The collection of data that is not relevant or necessary for the purpose of the collection might constitute an infringement of privacy and violation of the provisions of the law. It is expected that public entities that are subject to the principles of administrative law and the duty of proportionality observe these principles strictly.

B. Public entities receiving data in accordance with the provisions of the Data Transfer between Public Entities Regulations are obligated to delete excess data immediately after its reception.

C. The PPA recommends to all relevant entities to integrate the data minimization principle within the framework of their activity. According to this principle, it is necessary to avoid storage and any additional use of data that is not necessary for the purpose for which it was collected and for the purpose of the database in which it is stored. Therefore, it is necessary to store only the minimal data required for these purposes. This is relevant to the scope of the data, its type, its sensitivity and the like. The storage of data not in accordance with the purpose for which it was provided or the purpose of the database, or associated purposes essential for accomplishing the said goals (e.g. litigation purposes or a statutory duty to keep the data) increases the risk of privacy infringement and violation of data security duties, and it is recommended to avoid such actions.

D. The database owner (controller) is obligated to review annually whether the data stored in the database exceeds what is required for the database purposes. The PPA's approach is that there are circumstances in which it is preferable that such an inspection be conducted a few times during the year, for the purpose of avoiding storing excess data for a long period of time without justification. As long as the data stored in a database includes sensitive personal data on a large scale, and there is difficulty in justifying the continued retention of the data over time (in relation to the purpose of the database or its collection), it is recommended that the database owner (controller) examined whether his database stores excess data more frequently than required by the Regulations.

E. In circumstances in which a database owner (controller) reaches the conclusion that certain data stored in his database is excess data, and does not take action for minimizing it, such conduct could constitute a violation of Article 2(c) of the Data Security Regulations, and the database owner (controller) might be exposed to legal action.

F. In specific circumstances in which there could be a statutory duty to minimize excess data – e.g. following a request for the correction or deletion of data according to Article 14 of the Privacy Protection Law – the relevant entities are required to take action for the purpose of minimizing the data at the earliest opportunity in accordance with the provisions set forth in the law.

G. The PPA wishes to emphasize that conducting a Privacy Impact Assessment in an early stage of the data systems design is an efficient and effective way to minimize the risk of infringement of privacy, and lead to minimization in the collection and storage of excess data[17]. The preparation of such assessment is part of a broader perspective of Privacy by Design. The PPA would also like to emphasize the benefit in the appointment of a Privacy Protection Officer who will also function, *inter alia*, as the proper and efficient party to examine the steps the organization has taken for minimizing the risk of infringement of privacy[18].

[17] For a template of 'Privacy Impact Assessment' published by the Privacy Protection Authority see: https://www.gov.il/BlobFolder/generalpage/privacy_by_design/he/privacyimapctassessment2015.pdf

[18] See the draft for public hearing on the "Appointment of a Privacy Protection Officer in an organization and their duties" published by the Privacy Protection Authority: https://www.gov.il/BlobFolder/rfp/refrences_dpo/he/DPO.pdf

Conclusion

In the present digital reality large amounts of data that are collected and stored in databases are in fact considered as excess data that is unnecessary and irrelevant for the purpose which they were initially collected for, or for the purposes of the database in which they are stored. The minimization of excess data can result in the minimization of the infringement of privacy.

In this document the Privacy Protection Authority reflected the relevant provisions of the law and presented recommendations to minimize the collection and storage of excess data in databases. **In general, the PPA recommends all relevant entities to integrate the principle of data minimization within the framework of their activities, in order to avoid from keeping personal data unnecessary for the collection or database purposes, and store only the minimum data necessary for these purposes in terms of the scope of the data, its type and the like**. As stated in this document, such an approach is consistent with different requirements laid down in Israeli law, such as Article 2(9) and Article 8(b) of the Law, and in Article 2(c) of the Data Security Regulations.

The PPA would like to emphasize that the storage of excess data constitutes a risk of privacy infringement and might often contradict the interests of corporations holding the data. However, the PPA would like to clarify that data that is no longer required for the collection or database purposes, but its retention is required as a derivative of these purposes (such as data required for future litigation), as well as data collected in accordance with a statutory duty, does not constitute as excess data for this document.