The New EU General Data Protection Regulation[1]

Dear clients and friends,

On 14 April 2016 the EU Parliament formally approved the General Data Protection Regulation ("**the Regulation**"). The Regulation will dramatically change the current EU data protection regulatory framework, which is currently based on Directive 95/46/EC ("**the Directive"**).

The Regulation is designed to **harmonize national data protection laws across the EU** and to **reinforce data protection rights of individuals**. It will be **directly applicable across the EU**, without the need for re-implementation by the individual Member States.

Although the Regulation will formally enter into force 20 days following its publication in the EU Official Journal, its provisions will take effect **after two years** (i.e., in **May 2018**), in order to allow companies, which **handle the personal information processing of European data subjects,** to have sufficient time to comply with the new regime and implement the **significant required adjustments to their own information practices**.

The consequences of non-compliance with the new Regulation may result in fines of up to €20 million or 4% of the company's annual global turnover.

This Client Update is intended to assist in **understanding the main changes set out in the Regulation**, as well as to assist in **mapping the next steps that should be taken by companies** in order to be prepared for this Regulation. It should be noted that this update does not constitute an exhaustive summary of the applicable changes and requirements, but rather only focuses on the key practical implications arising from the Regulation.

[1] Since we are not licensed to practice law outside of Israel this document is intended to provide only a general background regarding this matter. This document should not be regarded as setting out binding legal advice, but rather only a practical overview which is based on our understanding of the practical interpretation of the applicable laws, regulations and industry guidelines.

Asia House, 4 Weizmann St., Tel-Aviv 6423904, Israel | Tel: (972)-3-692-2020 | Fax: (972)-3-696-6464
Twitter: @hfnlaw | Blog: unfolding.co.il | hfn@hfn.co.il | www.hfn.co.il

We encourage all of our clients to take **the appropriate steps to address the legal requirements stemming from the Regulation**, and we would be glad to assist in advising on the steps to be taken for its implementation.

THE MAIN CHANGES SET OUT IN THE REGULATION

Territorial Scope

- **Broader territorial reach**

  The Regulation will have a broader territorial reach than the Directive.

  The Directive applies to non-EU data controllers (i.e. entities that have the capacity to determine the purposes and the means of processing the personal information) if they process personal information within the context of their establishment's activities in the EU or make use of equipment in the EU to process data.

  The Regulation, however, will apply to both **data controllers** and **data processors** (i.e. entities that process personal information on behalf of a data controller) without having an establishment in the EU, **if their processing activities relate to offering goods or services to data subjects in the EU or to the monitoring of their behavior**.

  Data controllers and data processors without an establishment in the EU will be required to designate a **formal representative** in the EU. The representative shall be mandated to be addressed, in addition to or instead of the data controller or the data processor, on all issues relating to the processing of personal information under the Regulation.

  In practice, companies established outside the EU should consider whether their data processing activities expose them to the EU data protection laws. If so, companies will need to consider the appointment of a formal representative and address the legal requirements, which are stipulated under the Regulation.

Asia House, 4 Weizmann St., Tel-Aviv 6423904, Israel | Tel: (972)-3-692-2020 | Fax: (972)-3-696-6464
Twitter: @hfnlaw | Blog: unfolding.co.il | hfn@hfn.co.il | www.hfn.co.il

Regulatory Supervision and Corporate Governance

- **Supervisory Authorities**

  While the original purpose of the Regulation was a "one-stop-shop" concept that would simplify the interaction of companies with various Data Protection Authorities ("**DPA**"), the Regulation sets out a somewhat complex mechanism, involving a one "lead" DPA and other "concerned" DPAs. The lead DPA would be the DPA with jurisdiction over the company's **main establishment**. Where a specific processing activity affects data subjects in more than one Member State, then the lead DPA is required to consult with all other "concerned" DPAs. This will change the current legal regime under the Directive, which empowered national DPAs to enforce the Directive, as implemented under the Member States' national regulations.

  In practice, the lead DPA will supervise all of the data processing activities of the company and shall be responsible for overseeing all supervisory and enforcement actions across other EU Member States, with the assistance and oversight of "concerned" DPAs in other relevant EU Member State.

- **The European Data Protection Board**

  Pursuant to the Regulation, the new European Data Protection Board ("**EDPB**") will be established and replace the current Article 29 Data Protection Working Party, which was established under the Directive. The EDPB will have **broader powers** than the advisory Article 29 Working Party and will be able to adopt **binding decisions**. For instance, the EDPB may issue **guidance on the implementation of appropriate practical measures for compliance with the Regulation**.

- **Data Protection Officer appointment**

  Under the Regulation, both data controllers and data processors of personal information **must appoint a Data Protection Officer** ("**DPO**") who will have an expert knowledge of data protection regulations, in any case where the **core activities** of the company require **regular and systematic monitoring of data subjects on a large scale**, or where the core activities of the company consist of processing data on a **large scale of special categories** (such as sensitive data). The DPO should advise the company on its compliance obligations; monitor compliance with the obligations; and act as a contact point for data subjects and DPAs.

  In practice, companies should consider if they are obliged to appoint a DPO under the Regulation. In the case where this appointment is required, companies must identify a

suitable person to fulfill this role and define his/her scope of responsibility in the company.

- **Internal records to replace registration requirements**

  Under the Directive, data controllers are required to register with the relevant supervisory authority before carrying out processing activities of personal information. In this regard, while each Member State has applied different requirements, many have included a requirement to provide the supervisory authority with a summary of data processing activities.

  In place of registration, the Regulation will require data controllers to maintain **internal records** which cover their processing activities. These records shall contain **detailed information**, including: details of the data controller; the purpose of the processing; the categories of recipients to whom the personal information have been disclosed; a description of categories of data subjects and of the categories of personal information; transfers of personal information to a third country; a general description of the technical and organizational security measures, etc.

  Data processors will also be required to maintain internal records with regard to their data processing activities. These records shall include the details of each controller, on behalf of which the processor is acting; the categories of processing carried out on behalf of each controller; transfers of personal information to a third country, etc.

  Upon written request, both data controllers and data processors are required to make their records available to the relevant DPA.

  In practice, companies should facilitate and maintain updated detailed records which specify their data processing activities, as stipulated under the Regulation.

Accountability and Procedural Obligations

- **Requirement to "demonstrate compliance"**

  The Regulation explicitly requires **data controllers and data processors to "demonstrate compliance"** with data protection principles by **implementing appropriate technical and organizational measures**, and to ensure a level of protection appropriate to the risk.

The Regulation refers to various tools which may help demonstrate compliance, such as **codes of conduct, seals or certifications**. The Regulation further elaborates on actions that may need to be taken by both data controllers and processors in this matter, including encrypting or pseudonymising of personal information; ensuring the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal information; testing, assessing and evaluating the effectiveness of security measures; etc.

In practice, companies will need to practically implement up to date technical and organizational protection policies and measures in order to demonstrate and ensure that personal information is being processed and used in the appropriate manner.

- **Increased obligations for Data Processors**

Under the Directive, the primary obligation to comply with data protection legislation falls on the data controllers. Consequently, the data controller is obliged under the Directive to impose contractual obligations on the data processors with regard to their use of personal information.

Unlike the Directive, **the Regulation will also impose direct statutory obligations on data processors**, such as implementation of appropriate technical and organizational security measures to secure personal information; the obligation to notify data controllers of data breaches; complying with the requirements of the Regulation with regard to the transfer of personal information from the EU; etc.

In addition, data processors and data controllers may be held **jointly liable for damages** (i.e. each of them will be responsible for the entire damages) caused by their processing activities.

In practice, data processors may need to review their processing practices and their data processing agreements in order to ensure their compliance with the new regulatory obligations.

- **Data Protection Impact Assessment (DPIA)**

Under the Regulation, data controllers are required to **conduct a data protection impact assessment (DPIA) in the case where data processing activities present high risks to data subjects' rights**. The DPIA is designed to assess the privacy risks and the measures which are taken to address those privacy risks.

The Regulation provides an open list of processing activities that require DPIA, including the processing of special categories of personal information (e.g. racial or ethnic origin; political opinions; religious or philosophical beliefs; health or sex life; sexual orientation; etc.) and systematic evaluation of personal aspects by automated processing, including data profiling (i.e. processing personal information in order to analyze or predict any feature of the data subject's behavior, preferences or identity).

In practice, companies should consider conducting a DPIA, where appropriate, with respect to their processing activities.

- **Privacy by default and by design**

The Regulation states that data controllers must implement appropriate technical and organizational measures, which meet **the principles of privacy by design and privacy by default**.

The measures should ensure that only personal information which is necessary for each specific purpose of the processing is processed. This applies to the amount of information being collected, the extent of their processing, the period of their storage and their accessibility. In this context, the Regulation encourages companies to pseudonymize (i.e depersonalize) personal information where possible. Similarly, when developing applications and products that process personal information, privacy settings on these applications and products should protect data subjects by default.

In practice, companies will need to take privacy requirements into account both at the time of the determination of the means for processing personal information and at the time of the processing itself.

Substantive Requirements and Rights

- **Legal grounds of data processing**

Under the Directive, the data subjects' informed consent is one of the main legal bases for any collection, use or process of their personal information. The way in which consent is to be given by data subjects should be specific, informed and unambiguous with respect to any processing of personal information.

The Regulation makes valid consent more difficult to obtain. In this regard, the Regulation states that consent must be conveyed by **a clear affirmative action or a statement made by the data subject**. Accordingly, silence, pre-ticked boxes or inactivity should not constitute consent. When the processing has multiple purposes, **consent should be granted specifically for all of the processing purposes**. The Regulation also states that if the data subject's consent is given in the context of a written declaration, which also concerns other matters, the request for **consent must be presented in a manner which is clearly distinguishable from the other matters**.

Another basis for legitimate processing of personal data under the Directive was the "**legitimate interests**" of the data controller. This basis will continue under the Regulation to be a legal basis to process (non-sensitive) personal data, with the company's interests still being balanced against the rights of the individual. However, unlike the Directive, the Regulation emphasizes the importance of the **reasonable expectations of the individual at the time of collecting data**.

Similarly to the Directive, the **purpose principle**, according to which the processing of personal information is only allowed for the purposes for which it was legitimately collected, continues to apply under the Regulation.

In practice, companies which rely on a data subject's consent in order to collect or process personal information, will need to carefully review their practices in order to ensure they are being granted in accordance with a valid consent by the data subject for the processing of personal information. Companies which rely on the more narrowly interpreted "legitimate interests" basis will need to carefully review the basis for such processing against the increased weight of the data subject's interests.

- **Data subjects' rights**

Data subjects are guaranteed certain rights in relation to the collection and use of their personal information, such as the **right of access, rectification, erasure** and **objection**. Under the Regulation, those rights will continue to apply (subject to minor changes) and several **new rights** are being explicitly stipulated:

  - **The right of data portability** means that data subjects will have the right to receive their personal information from a data controller in a machine-readable format and to have the data transmitted to another data controller, where technically feasible.
  - **The right to be forgotten** means that data subjects have the right to demand that companies shall delete or destroy their personal information on various grounds (for example, where

the information is no longer needed for its original purpose; or where the data subject has withdrawn its/his/her consent for the processing of the data and there is no overriding, countervailing interest).

- **The right to restriction** means that data subjects will have the right in some cases to demand that the further processing |(other than storage) of their personal information may be suspended, such as when the accuracy of the data is contested; or the processing is unlawful; or the data is no longer needed for the purposes of the processing.

In practice, companies may need to adjust their data processing practices in order to provide these rights to their data subjects.

- **Profiling**

The Regulation adds a new requirement, by which data subjects have the right not to be subjected to the automated processing of personal information which is intended to analyze their preferences or assess their future behavior and habits ("**Profiling**").

In order for a Profiling to be allowed, it is necessary to obtain the data subject's **affirmative and explicit consent to the Profiling**, to notify the data subject that Profiling is taking place and provide information regarding the significance and consequences of the specific Profiling.

Under the Regulation, **Profiling performed solely on the basis of "sensitive data"** (personal information which may reveal the data subject's race, ethnic origin, political opinions, religion, genetic data, health data, sex orientation, and more) **is prohibited**.

In practice, companies which engage in the Profiling of personal information must review their consent mechanism, provide notifications with regard to Profiling and incorporate the new requirements and restrictions in order to be in compliance with the new Regulation.

- **Data processing notifications**

Companies are required to provide information to data subjects about their data processing activities.

The Directive elaborates certain elements that must be conveyed to the data subjects, such as the identity of the data controller; the purposes of processing; recipients of the data; and the data subject's rights.

The Regulation contains a more detailed list of mandatory elements that should appear in data protection notices, including the contact details of the organization's DPO (if applicable), the legal basis which the organization relies upon to process personal information, information on cross-border data transfers and data retention periods.

In practice, companies should review and revise their current information and privacy policies in order to identify and complete missing elements which are required under the new Regulation.

- **Children's' personal information**

In relation to the offering of services directly to children, the Regulation imposes new restrictions on the collection and use of personal information of children **under 16 years of age** (Member States may lower the threshold to 13 years of age) and which require **parental consent** for the processing. The data controller is obliged to make reasonable efforts to verify in such cases that consent is given or authorized by the parent.

In addition, in the event where personal information of children is being processed, the information regarding the process should be set out in **clear and plain language that the child can easily understand**.

In practice, companies that collect or use personal information of children or develop applications and services, which enable the collection of such information should address these new restrictions, in order to ensure compliance with the Regulation.

- **Cross-border transfer**

The Directive restricts the ability of data controllers and data processors to transfer personal information outside of the European Economic Area. Data transfer is allowed, inter alia, to countries that were recognized by the European Commission as providing an adequate level of privacy protection, where the data subject has unambiguously consented to it or where the transfer is made pursuant to an appropriate organizational and contractual mechanism that ensures an adequate level of data protection.

The new Regulation preserves the exiting transfer restrictions and encourages the use of binding corporate rules (BCRs) and model contractual clauses. As certain existing authorization requirements that were included in the Directive have been removed from the Regulation, using these transfer mechanisms should become easier. The Regulation

also allows using other instruments for cross-border transfer of personal data, such as **recognized codes of conduct and seals**.

The Regulation elaborates on the elements that the European Commission must take into account when assessing the adequacy of non-EU jurisdictions. Member States are authorized to expressly restrict the transfer of specific categories of personal information, for important reasons of public interest.

In practice, companies should review their current data transfer practices, channels and agreements and consider whether they comply with the data transfer restrictions.

- **New data breach notification requirements**

The Regulation sets out a **new general obligation on companies to report data breaches to the DPA and to the affected data subjects**.

Data controllers will be obliged to notify the DPA of a data breach without undue delay and, where feasible, no later than 72 hours after having become aware of it, unless the breach is unlikely to result in a risk for the rights and freedoms of individuals. Data controllers must notify data subjects of a breach where it creates a high risk to the rights and freedoms of individuals without undue delay, although some exceptions may apply (e.g. when implementing appropriate data protection measures).

Infringements of the data breach provisions shall be subject to administrative fines of up to €10 million or up to 2% of the annual turnover of the preceding financial year, whichever is higher.

In practice, companies must address data security practices in order to prevent and detect data breach attempts and implement a comprehensive data breach response plan in order to react promptly in the event of a data breach.

NEXT STEPS

Although the Regulation will not have direct effect until the spring of 2018, **companies should start preparing for the new regulatory framework.**

In addition to the Regulation, the European Commission has the power to adopt further rules to specify further detailed issues under the Regulation in various limited cases, such as the **criteria and requirements for certification mechanisms**, **data protection seals and marks**, **information to be presented by standardized icons**, and procedures for providing such icons. The EDPB may issue additional guidance on the **implementation of appropriate practical measures** for compliance with the Regulation, such as guidance on Profiling, using personal data for Big Data purposes and more.

In practice, companies should review their current data collection practices and examine the specific challenges they are facing under the new regime. Consequently, companies may need to adapt the ways they collect, use and process personal information, to build and implement the appropriate governance policies and to thoroughly address the security aspects of the personal information collected by them.

Specifically, companies would need to:

- ✓ Consider whether their data processing activities expose them to the new territorial scope under the Regulation and consider the appointment of a **formal representative**, where applicable.
- ✓ Consider whether they are obliged to **appoint a Data Protection Officer (DPO)**, and if so, to properly define its **authority and the areas of responsibility within the organization**.
- ✓ Put in place and maintain **internal records**, which consist of detailed information regarding their processing activities.
- ✓ Put in place and maintain **up to date technical and organizational data protection policies and measures**.
- ✓ Revise and amend, where needed, **current agreements with third parties** in order to ensure their compliance with the new obligations which apply to both data processors and data controllers.
- ✓ **Implement up to date technical and organizational security measures** in order to ensure that personal information is being processed and used in a secure manner.

- ✓ Consider **conducting a Data Protection Impact Assessment (DPIA)** where appropriate.

- ✓ Update internal **development and operational procedures to include privacy by design and by default requirements**, both at the time of the determination of the means for processing personal information and at the time of the processing itself.

- ✓ **Address organizational data security and implement a data breach response plan** in order to react promptly in the event of a **data breach**.

- ✓ Update privacy practices which relate to the legitimacy of collecting personal information, such as obtaining data subjects' **affirmative consent** or reassessment of the applicable "**legitimate interests**" that form the legitimacy of the processing.

- ✓ Review and adjust data processing practices in order to **provide data subjects with the expended data subjects' rights**.

- ✓ Review and adjust **Profiling practices** and address the applicable consent and notifications requirements, as well as the applicable restrictions on Profiling.

- ✓ Review and adjust current **privacy notices** in order to identify and complete **missing information and procedures** which must be addressed under the new Regulation.

- ✓ Determine the need to put in place **a valid mechanism in order to obtain parental consent** and comply with other restrictions on the collection and use of **personal information of children under 16 years of age**.

- ✓ Review current **cross-border data transfer practices**, including current agreements with data importers and data exporters, and consider whether they comply with the data transfer restrictions.

HFN ADTECH AND TECHNOLOGY COMPLIANCE TEAM

Globally recognized for our expertise and proficiency in the Tech Regulation and Compliance ecospheres, we advise startups, multi-national companies, mobile apps and software developers on regulatory and compliance matters surrounding privacy and data protection, e-Commerce, adtech and media, data and technology compliance. Our thorough knowledge and diverse experience with the increasing volume of regulations, enforcement actions and legislative trends in a myriad of jurisdictions, as well as with the industry's best practices and leading self-regulatory guidelines, enables us to offer unique and practical solutions for often complex situations and assist in the development, implementation and management of adequate procedures, the goal of which is to mitigate legal and business risks.

OUR TEAM LEADERS

Gil White | White@hfn.co.il
Gil is the head of HFN's Internet and E-Commerce department, and has a diversified practice with a concentration in finance and e-commerce. Gil has, for over a decade, advised the world's leading internet gaming, forex and other e-commerce companies with respect to corporate and other issues.

Ariel Yosefi | Yosefia@hfn.co.il
Ariel heads the Adtech and Technology Compliance practice at HFN and is highly regarded for his global experience in advising multinational companies, mobile app and SDK developers, ad networks, ad exchanges, software vendors, startups and others, on regulatory and compliance matters surrounding app-compliance, e-Commerce, monetization, Adtech and online data protection. Ariel also specializes in worldwide regulatory frameworks surrounding online gaming and advises leading companies on regulatory and compliance matters.

Dr. Nimrod Kozlovski | Kozlovskin@hfn.co.il
Nimrod is a partner at HFN and leads the firm's Cyber and Internet law practice. Nimrod is an expert investor in Cyber Security and a teaching professor on Internet and Cyber Law, Information technology and innovation. Nimrod received his doctor degree in law (J.S.D) from Yale Law School and conducted his Post-Doctorial research in computer science on proactive security at the Yale School of Computer Sciences. Nimrod is also a Partner at JVP, a leading Israeli VC, focusing on Cyber Security and Big Data, and has formerly founded innovative start-ups.

Ido Manor | Manori@hfn.co.il
Ido is a member of the HFN's Adtech and Technology Compliance team, and specializes in advising Israeli and international clients, startups and internet companies, on a wide range of regulatory and commercial matters involving data protection and privacy, online advertising, user generated content, social media and mobile marketplaces compliance, e-commerce and international trade.

Hilla Himel | Himelh@hfn.co.il
Hilla is a member of the HFN's Adtech and Technology Compliance team, and specializes in advising Israeli and international clients, startups and internet companies, on a wide range of regulatory and commercial matters involving data protection and privacy, download and install, online advertising, media and traffic, social media and mobile marketplaces compliance.

Dr. Avishay Klein | Kleinav@hfn.co.il
Avishay is a member of the HFN's Adtech and Technology Compliance team, and specializes in advising on a wide range of regulatory and commercial matters involving worldwide regulatory and practical aspects of cyber security, data protection and privacy, online advertising, mobile marketplaces compliance and international trade.