

A Regional Guide to Employee Data Privacy

EMEA

Introduction

Data privacy is a priority for all employers but especially those with operations in more than one country. It impacts all aspects of the employment relationship and, with the increase in data transfers between businesses and across borders, employers often need to comply with multiple laws to minimize the risk of significant fines and liabilities.

A Regional Guide to Employee Data Privacy is designed to help employers navigate the specific, and increasing, challenges of handling employee data in different jurisdictions. Covering 24 key countries, the guide contains the following:

- **Key Questions & Answers** – covering applicant and employee personal data, privacy statements and policies, retention periods for employee data, transfers of employee data overseas and to third parties, sanctions for breach and potential pitfalls for employers;
- **GDPR Overview** – highlighting the major changes and requirements introduced by the new European General Data Protection Regulation (“GDPR”), affecting businesses both within and outside the European Union; and
- **“In Brief” and “In Detail” Guidance** – providing both quick reference and more detailed content across all jurisdictions.

We hope that you will find this publication useful. It has been compiled by lawyers from a major international law firm as well as partner law firms in other jurisdictions.

USER GUIDE 



HOME



GDPR
OVERVIEW



COUNTRIES

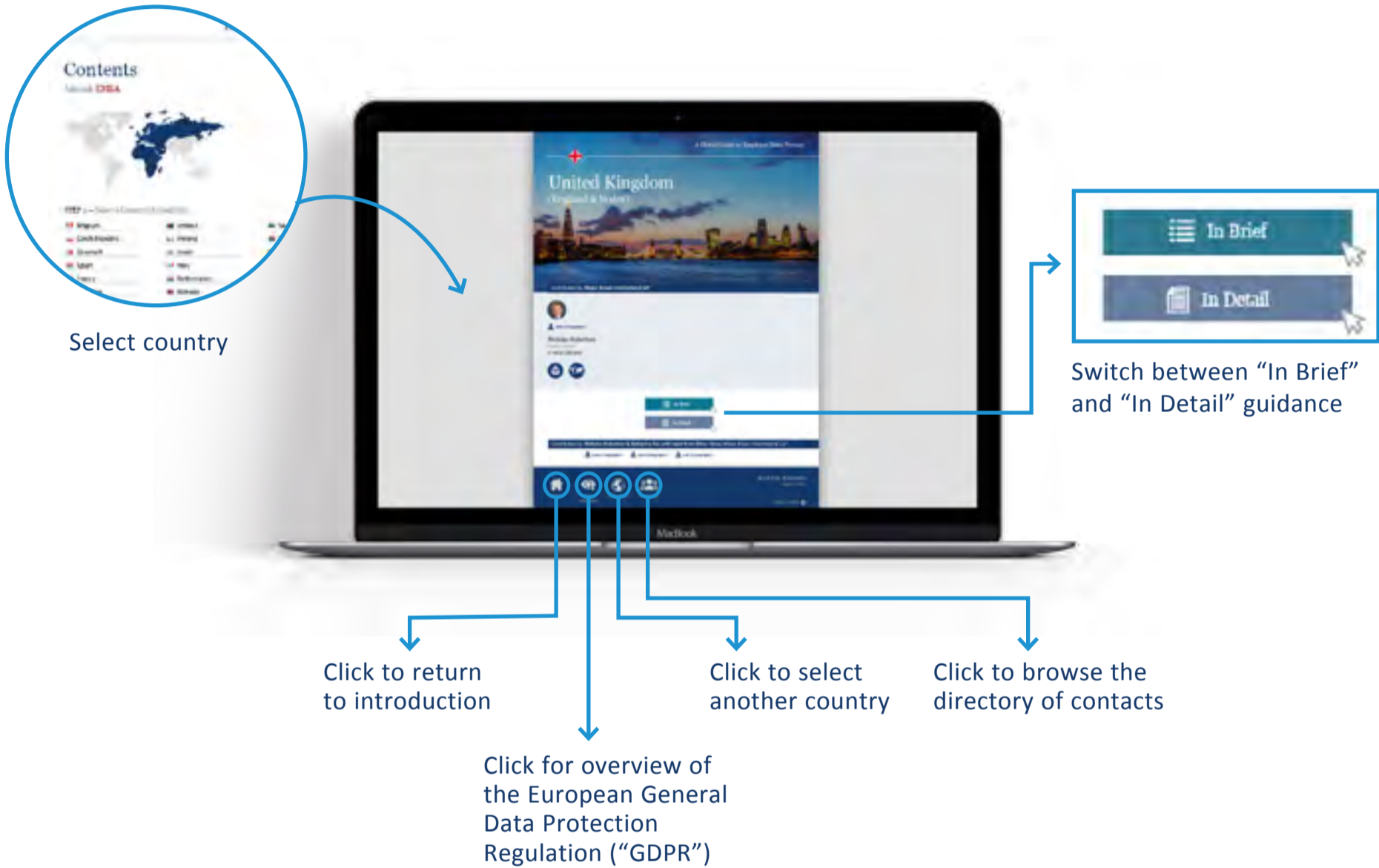


DIRECTORY

August 2018

SCROLL DOWN 

User Guide



HOME



GDPR OVERVIEW



COUNTRIES



DIRECTORY

GDPR Overview

The new European General Data Protection Regulation¹ (“**GDPR**”) came into force throughout the European Union (“**EU**”) on May 25, 2018. Unlike previous European data protection legislation, the GDPR does not require implementing national legislation, but is directly applicable. It introduces significant changes and additional requirements that will have a wide-ranging impact on employers both within and outside the EU.

Key Changes and Additional Requirements

- **European data protection law can now apply worldwide** – The GDPR covers not only the processing of personal data by an establishment of a controller or processor in the EU, regardless of whether the processing takes place in the EU, but also organizations outside of the EU insofar as their data processing activities are related either to offering goods or services to EU individuals, or to monitoring their behavior within the EU.
- **Tougher sanctions** – The maximum fine for a breach of the GDPR has been substantially increased to a maximum of 4% of an enterprise’s worldwide turnover, or EUR 20 million per infringement, whichever is higher.
- **A new data breach notification obligation** – Organizations now have to notify the relevant data protection authority of a breach without undue delay and where feasible within 72 hours. A notification must also be made to the individuals affected without undue delay where there is a high risk to their rights and freedoms.
- **New data privacy governance, record of processing activities and impact assessment requirements** – Many organizations now need to appoint a data protection officer to be responsible for implementing and monitoring that organization’s compliance with the GDPR and to carry out assessments of the organization’s data processing. Organizations are now also required to maintain a record of their processing activities and undertake data protection impact assessments for higher risk processing.
- **A requirement to implement “privacy by design” and “privacy by default”** – Businesses must now take a proactive approach to ensure that data protection is already integrated when technology is created and implemented, and that an appropriate standard of data protection is the default when personal data is being processed.

¹The full text of the GDPR is available [here](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN

GDPR Overview (continued)

- **Stronger rights for individuals** – Employees now have the following rights, and organizations will need to determine how they will enable their employees to exercise them:
 - **Access and information:** Employees can request a copy of the personal data their employers hold about them, and must be informed of, among other details, the purposes of processing, the categories of personal data concerned and the recipients to whom the data will be disclosed.
 - **Rectification:** Employees can request correction of any incomplete or inaccurate information.
 - **Erasure (right to be forgotten):** Employees have the right to request deletion or removal of their personal data if they have been processed unlawfully, are no longer needed for their original or another lawful purpose, have to be erased for compliance with a legal obligation, or if the employee has withdrawn his/her consent or exercised his/her right to object to processing.
 - **Objection to processing:** If the employer relies on legitimate interests for processing, the employee can object to this processing on grounds relating to his/her particular situation.
 - **Restriction of processing:** Processing needs to be restricted if the employee contests the accuracy of the data, if the processing is unlawful or if the employer no longer requires the data for their original purpose, but the employee needs them for the establishment, exercise or defense of legal claims.
 - **Data portability:** Employees can request a copy of their personal data in a machine-readable format in order to transfer them to another recipient. Where technically feasible, the employer can also be required to carry out the transfer directly.
- **Enhanced requirements for the supply chain** – Businesses must only use other parties to process personal data that provide sufficient guarantees that they will implement appropriate security measures to satisfy the requirements of the GDPR. These service providers will now be held accountable for their own level of appropriate security, must document their processing to the same extent under the GDPR and must obtain prior consent to employ sub-processors. Existing contracts with third parties therefore need to be reviewed and are likely to require amending.
- **One-stop shop principle** – For organizations operating in more than one EU Member State, the GDPR implements a so-called one-stop shop principle. Such organizations will be able to liaise with one data protection authority (the “**lead authority**”). The lead authority is tasked with coordinating actions regarding the cross-border activities, thereby closely involving other authorities.



HOME

GDPR
OVERVIEW

COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN

GDPR Overview (continued)

In addition, particular areas of concern for employers are:

- **Processing and consent** – The GDPR enhances the requirements for a valid consent. It needs to be given freely, be specific, informed and unambiguous, and must take the form of an affirmative action or statement. In addition, data subjects have the right to refuse and to withdraw their consent at any time. In principle, consent can also be the legal basis for data processing in an employment situation. However, due to the imbalance of power between employer and employee, it may be questionable whether the consent was voluntary; often, employees will feel that they have no option but to consent.
- **Special categories of personal data** – Some special categories of personal data (“sensitive data”) are more closely protected. This is information that relates to someone’s race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, health, sex life and sexual orientation, and genetics/biometrics. In addition to the requirements described above, consent to the processing of these categories of data must be explicit, making it even more difficult for employers to rely on consent.
- **International transfers of data** – Cross-border data transfers may only take place if the transfer is made to an “adequate jurisdiction,” or if appropriate safeguards have been provided. Third countries (i.e., countries outside the European Economic Area (“**EEA**”)) can be determined “adequate” if the European Commission finds that they ensure an adequate level of data protection. Such an adequacy decision has, in particular, been adopted with regard to the EU-US Privacy Shield framework, thus allowing data transfers to US companies that have self-certified under the Privacy Shield. A transfer to countries lacking this status requires a lawful data transfer mechanism, such as standard contractual clauses adopted by the European Commission, or binding corporate rules that have been approved by the competent data protection authorities.

While many employers have taken steps to ensure compliance with the GDPR, it will have a continuing impact on businesses both within and outside the EU.



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 


Contents

Select a Country/Jurisdiction

 [Belgium](#)

 [Czech Republic](#)

 [Denmark](#)

 [Egypt](#)

 [France](#)

 [Germany](#)

 [Greece](#)

 [Hungary](#)

 [Iceland](#)

 [Ireland](#)

 [Israel](#)

 [Italy](#)

 [Netherlands](#)

 [Norway](#)

 [Poland](#)

 [Russia](#)

 [Saudi Arabia](#)

 [South Africa](#)

 [Spain](#)

 [Sweden](#)

 [Switzerland](#)

 [Turkey](#)

 [United Arab Emirates](#)

 [United Kingdom](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Greece



Contributed by: **Bernitsas Law**

 In Brief

 In Detail

Contributed by: **Tania Patsalia**, Bernitsas Law

 [Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Greece

In Brief

1. Does employee data privacy law in your jurisdiction go beyond the GDPR?

In Greece, a draft bill implementing certain provisions of the GDPR (“**Draft Bill**”) – *inter alia* with regard to the processing of employee data in the employment context – was put into public consultation in early March 2018. Following this, an updated draft (not publicly available yet) is expected to be introduced soon to the Greek Parliament for discussion and adoption.

2. Is there a law regulating applicant personal data?

Under the Draft Bill, applicants are also treated as employees. In addition, and pending adoption of the Draft Bill, Directive 115/2001 of the Hellenic Data Protection Authority (“**HDP**A”), governing processing of personal data in the context of employment, includes provisions that are applicable to candidates. The general provisions of the GDPR also apply.

3. Is there a law regulating employee personal data?

Yes, apart from the Draft Bill and HDP A’s Directive (please see above), the current Greek Data Privacy Act is, until its replacement by the Draft Bill, the main legislation applicable to the protection of personal data in Greece. The general provisions of the GDPR also apply.

4. Do I need to have a privacy statement or agreement?

Employees must be properly informed in advance about the processing of their data in the employment context, in accordance with the GDPR requirements.

5. How long must I retain employee data? What is best practice?

Employee data should be kept for no longer than is necessary.

6. Can I transfer employee data overseas?

Yes, subject to appropriate safeguards being provided by the employer, in accordance with the GDPR requirements.

7. Can I transfer employee data to a third party?

The transfer of employee data to a third party is subject to the GDPR requirements and, under HDP A’s Directive, is permitted only for purposes directly related to the employment relationship or if the transfer arises from a statutory provision.

8. What are the consequences of breach?

Administrative and criminal sanctions may be imposed in the event of a breach. Damages may also be awarded.

9. What are the main pitfalls?

Draft Greek legislation has been formulated to cover the latest practices adopted/intended to be adopted by employers, such as processing of employees’ biometrics data, operation of CCTV in the workplace and use of geolocation tracking systems, which are permitted only under strict restrictions. There are also restrictions related to the processing of communications and monitoring employee use of the Internet.





Greece

In Detail

1. To what extent does employee data privacy law in your jurisdiction go beyond the GDPR?

In Greece, a draft bill implementing certain provisions of the GDPR (“**Draft Bill**”) was put into public consultation in early March 2018. Following this, an updated draft (not publicly available yet) is expected to be introduced soon to the Greek Parliament for discussion and adoption.

As the GDPR is directly applicable in Greece (as in all EU Member States), the Draft Bill applies to the processing of personal data in parallel with the GDPR, specifying, *inter alia*, the rules applicable to employees’ data processing and, in this regard, incorporating in essence the provisions laid down in existing guidelines issued by the Hellenic Data Protection Authority (“**HDP**A”) on those topics.

In particular, the Draft Bill specifies, among others, that:

- (a) employees also include candidates and former employees;
- (b) processing may, *inter alia*, be justified for the fulfillment of the employment relationship or on grounds of contract or law while, if the basis of the processing is employees’ consent, such consent must be in writing and given separately from the employment contract and employees must be free to revoke their consent without adverse effects;
- (c) special categories of data may only be processed based on contract or law;
- (d) data on criminal prosecutions, security measures and offenses may be processed where this is necessary to assess the employee’s qualifications for the specific job or to take a specific decision in the context of the employment;
- (e) CCTV in the workplace may be installed but only as an exception;
- (f) geolocation devices are allowed only for the protection of goods and persons or to ensure that the job has been performed where this is justified by the nature of the employment; and
- (g) monitoring employees’ communications in the workplace is permitted only where necessary for the protection of goods and persons or the organization and monitoring of the fulfillment of the employment, including checking expenses.

Employees must be individually and in writing informed about the processing of their data and the employer must have in place an internal regulation for the use of electronic communications in the workplace that should be made available

[HOME](#)[GDPR
OVERVIEW](#)[COUNTRIES](#)[DIRECTORY](#)

August 2018

SCROLL DOWN



Greece

In Detail

to the employees (and the employer must be able to prove this). It is noted, for the sake of completeness, that the relevant provisions under the Draft Bill essentially elaborate and expand further on the rules already set out in Directive 115/2001 of the HDPa governing processing of personal data in the context of employment (“Directive”).

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

The general provisions of the GDPR apply. Under the Draft Bill, applicants are also treated as employees. In addition, and pending adoption of the Draft Bill, the Directive also includes provisions that are applicable to candidates. The purpose of these provisions is to set out the boundaries within which the employer shall be entitled to lawfully collect, use and process employees’ as well as applicants’ data.

In this respect, the Directive provides that the employer, in its capacity as a controller, should collect the applicant’s personal data directly. If the applicant’s personal information is intended to be requested by a third party for the purpose of conducting a pre-employment check, the applicant must be informed in advance and must provide his/her explicit consent.

In any event, it is explicitly provided that the collection of applicant’s data should be restricted to what is absolutely necessary for the assessment of his/her suitability for the particular position. With regard to modern methods of personnel selection, such as through medical tests, it is stated that these should be performed only in exceptional cases and only if strictly necessary and appropriate for the fulfillment of a specific purpose directly related to the particular employment relationship in accordance with the principle of proportionality, and may be collected only following the applicant’s written consent, after he/she has been properly informed about the method, criteria, purposes and recipients of such data.

As regards the collection and further processing of information related to applicants’ criminal prosecutions and convictions, this is legally permissible only when justified by the particular job position (i.e., the employee will be handling money, etc.), as long as this is collected directly by the applicant.

Finally, with respect to the legal restrictions on the transfer of the applicant’s personal data overseas and/or to a third party, including to countries outside the EU/EEA, the GDPR provisions on the adoption of appropriate safeguards apply (please see question 6).



HOME

GDPR
OVERVIEW

COUNTRIES



DIRECTORY



Greece

In Detail

3. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee's personal data in your jurisdiction?

Apart from the Draft Bill, which is expected to be introduced soon to the Greek Parliament for adoption, and the Directive (please see analysis above), the current Greek Data Privacy Act (i.e., Law 2472/1997 on the protection of individuals with regard to the processing of personal data, as in force, implementing Directive 95/46/EC into Greek law) is, until its replacement by the Draft Bill, the main legislation applicable to the protection of personal data in Greece. There is also secondary regulation in the form of decisions and directives of the HDP. The general provisions of the GDPR also apply.

4. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

Employees, as data subjects, must be provided with adequate information, in clear and plain language, regarding the processing of their personal data in the employment context, in accordance with the GDPR requirements.

In addition, under the Draft Bill, the employer, as the controller, is under an obligation to set up internal regulations governing the use of communication and other electronic means by employees in the workplace or for business purposes. Such regulations should be disclosed to employees, and the employer should be in a position to prove that all employees have been made aware of the regulations.

5. For how long must an employer retain an employee's personal data? What is best practice?

Data should not be kept for longer than is necessary for the purposes for which the data are processed, in accordance with the GDPR principles. Therefore, if an employment relationship is terminated or the employee has not been recruited, the information should be kept in a form that permits identification of data subjects only for the period that is necessary for defending a claim before a court or a public authority. Holding information on a candidate whose application has been rejected should be at the candidate's request and with a view to the company considering the candidate for a position at a later stage.



HOME

GDPR
OVERVIEW

COUNTRIES



DIRECTORY



Greece

In Detail

6. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

The transfer of data outside the EU/EEA is subject to the legal restrictions under the GDPR. In this respect, the transfer of employees' personal data outside Greece, and, in particular, outside the EU/EEA, is subject to appropriate safeguards being provided by the employer, such as putting in place binding corporate rules or standard contractual clauses and on the condition that enforceable employees' rights and effective legal remedies for them are available.

7. What are the legal restrictions on transferring employees' personal data to a third party?

Under the Draft Bill, the collection and processing of employee personal data are only allowed for purposes directly related to the employment relationship or for purposes arising from a statutory provision. With regard to, in particular, the transfer of employees' data to a third party, this is only permitted for purposes directly related to the employment relationship or if the transfer is provided for under the law (subject also to the EU rules on the transfer of data to third countries) (please see Directive, p.20). As such, any transfer to a third party would need to be justified for specified purposes. Other members of the same group are also considered as third parties.

If employees' personal data shall be shared with a processor (e.g., a payroll provider), the employer should enter into a binding contract with the processor that meets the requirements set out in Article 28 of the GDPR.

8. What are the consequences of breaching privacy laws in your jurisdiction?

In the case of infringement of privacy laws in Greece, the administrative fines as provided for under the GDPR (i.e., amounting to up to EUR 20 million or up to 4% of the undertaking's total worldwide annual turnover of the preceding financial year, whichever is higher, depending on the type of infringement) may be imposed by the HDPa. In addition, the HDPa may also impose other administrative sanctions, such as warnings, reprimands or a ban on processing pursuant to the GDPR provisions.

Under the current Greek Data Privacy Act (until replaced by the Draft Bill), criminal sanctions, including fines and imprisonment, may also be imposed, and there are varying levels of fines and periods of imprisonment depending on the breach committed. The company's representative is liable to criminal sanctions where the controller is a legal entity. The infringer may be also liable to compensation for damages suffered, including moral damages.



HOME

GDPR
OVERVIEW

COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Greece

In Detail

9. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

With the coming into effect of the GDPR, rules and principles established by the HDPA in its directives or case law to date have been elaborated on and further expanded by means of the Draft Bill which is expected to be adopted soon.

Also, draft Greek legislation has been formulated to cover the latest practices adopted/intended to be adopted by employers, such as processing of employees' biometrics data, operation of CCTV in the workplace and use of geolocation tracking systems, which are permitted only under strict restrictions (i.e., when absolutely necessary for the protection of persons and goods in the workplace, taking into account the nature of the work, etc.).

There are also restrictions related to the processing of communications and monitoring employee use of the Internet. In particular, the collection and processing of data regarding communications in the workplace, including email, are only permitted where absolutely necessary for the protection of persons and goods in the workplace and for organizing and monitoring the completion of a particular task or cycle of work and especially for cost control purposes. The communication data processed should be restricted to that which is absolutely necessary and relevant in order to achieve these specified purposes. In this respect, employers are obliged to put in place internal regulations, of which the employees must acquire knowledge (in a proven manner).

In any event, an employer's obligation to provide employees with information regarding all aspects of the processing of their data in the employment context is taken particularly seriously by the HDPA, and compliance should be ensured in a proven manner at all times.

Contributed by: **Tania Patsalia**, Bernitsas Law

[Link to biography >](#)



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN

Directory

 **Belgium**



Nicolas Simon

Van Olmen & Wynant,
Avenue Louise 221, 1050 Brussels, Belgium



+32 2 644 05 11



nicolas.simon@vow.be



<http://www.vow.be/team.html>

 **Czech Republic**



Petra Sochorová

Havel & Partners,
Na Florenci 2116/15, Recepce A, 110 00 Prague 1 – Nové Město, Czech Republic



+420 255 000 111



petra.sochorova@havelpartners.cz



www.havelpartners.cz/en/team/counsel/73-counsel/32-petra-sochorova

 **Czech Republic**



Richard Otevřel

Havel & Partners,
Na Florenci 2116/15, Recepce A, 110 00 Prague 1 – Nové Město, Czech Republic



+420 255 000 111



richard.otevrel@havelpartners.cz



www.havelpartners.cz/en/team/counsel/73-counsel/41-richard-otevrel



HOME



GDPR
OVERVIEW




COUNTRIES



DIRECTORY

Directory

 Denmark



Tina Brøgger Sørensen

Kromann Reumert,
Sundkrogsgade 5, 2100 Copenhagen OE, Denmark




+45 70 12 12 11



tib@kromannreumert.com



en.kromannreumert.com/people/tina%20broegger%20soerensen

 Egypt



Sharif Shihata

Shalakany Law Office,
12 El Maraashly Street, Zamalek, Cairo, Egypt



+20 2 272 88 888



sshihata@shalakany.com



www.shalakany.com

 France



Julien Haure

Mayer Brown,
10 Avenue Hoche, 75008 Paris, France



+33 1 53 53 36 48



jhaure@mayerbrown.com



www.mayerbrown.com/people/Julien-Haure/



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

Directory

 France



Régine Goury

Mayer Brown,
10 Avenue Hoche, 75008 Paris, France



+33 1 53 53 43 40



rgoury@mayerbrown.com



www.mayerbrown.com/people/regine-goury/

 Germany



Dr. Guido Zeppenfeld

Mayer Brown LLP,
Friedrich-Ebert-Anlage 35-37, 60327 Frankfurt am Main, Germany



+49 69 79 41 2241



gzeppenfeld@mayerbrown.com



www.mayerbrown.com/people/dr-guido-zeppenfeld-llm/

 Germany



Björn Vollmuth

Mayer Brown LLP,
Friedrich-Ebert-Anlage 35-37, 60327 Frankfurt am Main, Germany



+49 69 79 41 1587



bvollmuth@mayerbrown.com



www.mayerbrown.com/people/Bjorn-Vollmuth/



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

Directory

 Germany



Vanessa Klesy

Mayer Brown LLP,
Friedrich-Ebert-Anlage 35-37, 60327 Frankfurt am Main, Germany



+49 69 79 41 1283



vklesy@mayerbrown.com



www.mayerbrown.com/people/Vanessa-Klesy

 Greece



Tania Patsalia

Bernitsas Law,
5 Lykavittou Street, GR-106 72, Athens, Greece




+30 210 361 5395



tpatsalia@bernitsaslaw.com



www.bernitsaslaw.com/lawyers/tania-patsalia/intellectual-property-data-protection-and-privacy=practices/

 Hungary



Péter Szemán

Bán, S. Szabó & Partners,
H-1051 Budapest, József Nádor Tér 5-6, Hungary



+36 1 266 3522



pszeman@bansszabo.hu



www.bansszabo.hu/en/team/dr-peter-szeman



HOME



GDPR
OVERVIEW



COUNTRIES




DIRECTORY

August 2018

SCROLL DOWN 

Directory

 Iceland



Áslaug Björgvinsdóttir

LOGOS Legal Services,
Efstaleiti 5, 103 Reykjavík, Iceland



+354 5 400 300



aslaug@logos.is



<https://en.logos.is/the-team/partners>

 Ireland



Ailbhe Dennehy

A&L Goodbody,
International Financial Services Centre, North Wall Quay, Dublin 1, D01H104, Ireland



+353 1 649 2000



ALGDublin@algoodbody.com



www.algoodbody.com/our-people/ailbhe-dennehy

 Israel



Revital Shprung-Levy

Goldfarb Seligman,
Ampa Tower, 98 Yigal Alon Street, Tel Aviv 67891, Israel



+972 3 608 9853



Revital.Shprung-Levy@goldfarb.com



www.goldfarb.com/our-attorneys/revital-shprung-levy



HOME



GDPR
OVERVIEW




COUNTRIES



DIRECTORY

Directory


 Israel

Gal Sion

Goldfarb Seligman,
Ampa Tower, 98 Yigal Alon Street, Tel Aviv 67891, Israel

 [+972 3 608 9853](tel:+97236089853)  Gal.Sion@goldfarb.com

 www.goldfarb.com/our-attorneys/gal-dayan-sion

 Italy

Francesco D'Amora

Quorum Studio Legale e Tributario Associato,
Via Cino del Duca 5, 20122 Milan, Italy

 [+39 02 87 21 32 37](tel:+390287213237)  fdamora@quorumlegal.com

 www.quorumlegal.com

 Netherlands

Hermine Voûte

Loyens & Loeff,
Fred. Roeskestraat 100, 1076 ED Amsterdam, Netherlands

 [+31 20 578 59 75](tel:+31205785975)  hermine.voute@loyensloeff.com

 <https://www.loyensloeff.com/en-us/our-people/hermine-voûte>



HOME



GDPR
OVERVIEW



COUNTRIES




DIRECTORY

August 2018

SCROLL DOWN 

Directory

 Norway



Christopher Sparre-Enger Clausen

Advokatfirmaet Thommessen AS,
Haakon VII's gate 10, 0116 Oslo, Norway



[+47 23 11 11 11](tel:+4723111111)



csc@thommessen.no



www.thommessen.no/en/people/partners/christopher-sparre-enger-clausen/

 Poland



Agata Szeliga

Sołtysiński Kawecki & Szlęzak,
Jasna 26, 00-054 Warsaw, Poland



[+48 22 608 70 06](tel:+48226087006)



agata.szeliga@skslegal.pl



www.skslegal.pl/en/zespol/agata-szeliga/

 Poland



Katarzyna Paziewska

Sołtysiński Kawecki & Szlęzak,
Jasna 26, 00-054 Warsaw, Poland



[+48 22 608 71 92](tel:+48226087192)



katarzyna.paziewska@skslegal.pl



www.skslegal.pl/en/zespol/katarzyna-paziewska/



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

Directory

 **Russia**



Markus Schaer

Secretan Troyanov Schaer SA,
Ulitsa Usacheva 33, Bldg. 1, 119048 Moscow, Russia




+74 95 232 03 01



markus.schaer@sts-law.ru



www.sts-law.ru/en/team_markus_schaer

 **Saudi Arabia**



Tom Thraya

Mayer Brown LLP,
Index Tower, Dubai International Finance Centre, Floor 11, Unit 1104, Dubai, United Arab Emirates



+971 4 375 7161



tthraya@mayerbrown.com



www.mayerbrown.com/people/Tahan-Tom-A-Thraya

 **Saudi Arabia**



Jad Taha

Mayer Brown LLP,
Index Tower, Dubai International Finance Centre, Floor 11, Unit 1104, Dubai, United Arab Emirates



+971 4 375 7166



jtaha@mayerbrown.com



www.mayerbrown.com/people/Jad-A-Taha



HOME



GDPR
OVERVIEW




COUNTRIES



DIRECTORY

Directory

 South Africa



Ross Alcock

ENSAfrica,

150 West Street, Sandton, Johannesburg, 2196, South Africa



+27 11 269 7600



ralcock@ensafrica.com



www.ensafrica.com/lawyer/ross-alcock?Id=320&searchterm=ross%20alcock

 Spain



Andrea Sánchez Guarido

Pérez-Llorca,

Paseo de la Castellana, 50, 28046, Madrid, Spain



+34 91 426 03 67



asanchez@perezllorca.com



www.perezllorca.com/en/lawyer/andrea-sanchez-2/

 Sweden



Åsa Gotthardsson

Advokatfirman Vinge KB,

Box 1703, SE-111 87, Stockholm



+46 10 614 30 00



asa.gotthardsson@vinge.se



www.vinge.se/en/our-people/asa-gotthardsson/



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

Directory

Switzerland



Christian Roos

Pestalozzi Attorneys at Law Ltd,
Loewenstrasse 1, 8001 Zurich, Switzerland



+41 44 217 91 11



christian.roos@pestalozzilaw.com



<https://pestalozzilaw.com/en/lawyers/christian-roos/>

Turkey



Irmak Dirik Erunsal

DAB Law Firm,
Poyracık Sokak, Feza Apt. No.18/7, Nisantasi Sisli, Istanbul, Turkey



+90 212 234 44 25



idirik@dablawfirm.com



www.dablawfirm.com/who-we-are

United Arab Emirates



Tom Thraya

Mayer Brown LLP,
Index Tower, Dubai International Finance Centre, Floor 11, Unit 1104, Dubai, United Arab Emirates



+971 4 375 7161



tthraya@mayerbrown.com



www.mayerbrown.com/people/Tahan-Tom-A-Thraya



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

 United Arab Emirates



Jad Taha

Mayer Brown LLP,

Index Tower, Dubai International Finance Centre, Floor 11, Unit 1104, Dubai, United Arab Emirates




+971 4 375 7166



jtaha@mayerbrown.com



www.mayerbrown.com/people/Jad-A-Taha

 United Kingdom



Nicholas Robertson

Mayer Brown International LLP,

201 Bishopsgate, London, EC2M 3AF, United Kingdom



+44 20 3130 3919



nrobertson@mayerbrown.com



www.mayerbrown.com/people/nicholas-robertson/

 United Kingdom



Katherine Fox

Mayer Brown International LLP,

201 Bishopsgate, London, EC2M 3AF, United Kingdom



+44 20 3130 3169



kfox@mayerbrown.com



www.mayerbrown.com/people/Katherine-Fox/



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY

Legal Statement

This publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

© 2018 Mayer Brown. All rights reserved.

Attorney advertising. Prior results do not guarantee a similar outcome.



HOME



GDPR
OVERVIEW



COUNTRIES



DIRECTORY