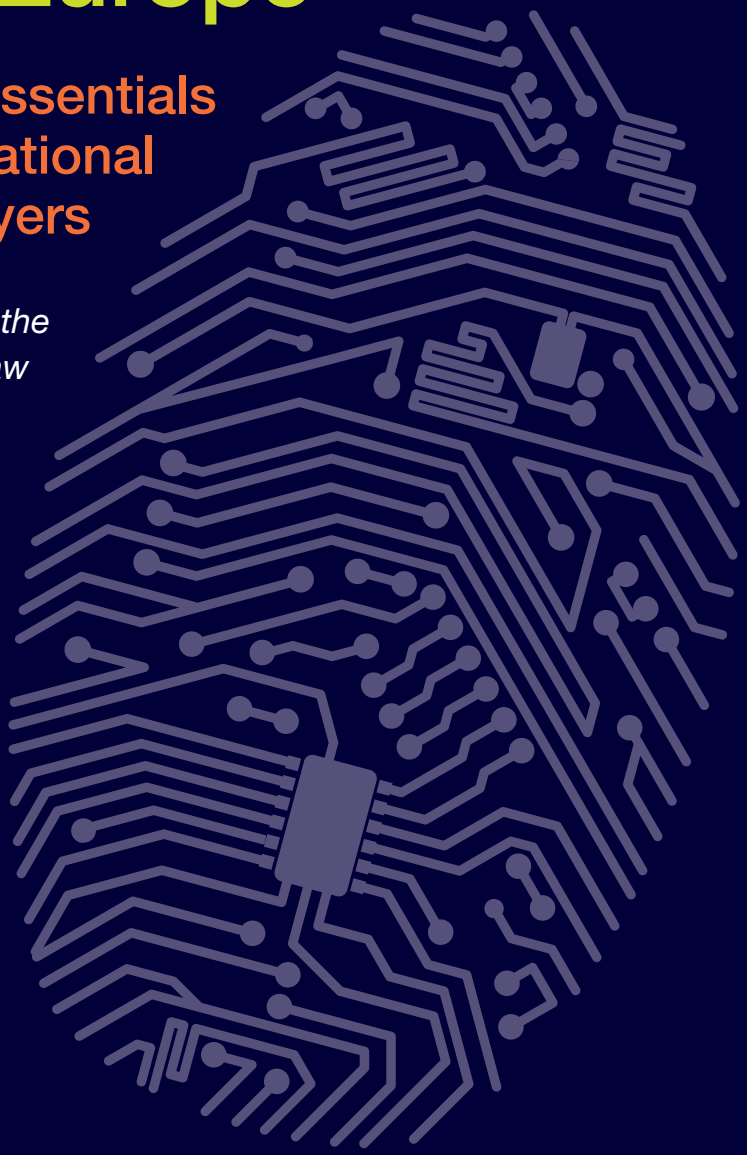
Employee Data Privacy in Europe

The Essentials for Multinational Employers

Prepared by the Employment Law Alliance



EMPLOYMENT LAW ALLIANCE®
Helping Employers Worldwide®
www.employmentlawalliance.com

NEOCLEOUS
www.neocleous.com

Andreas Neocleous & Co LLC

Andreas Neocleous & Co LLC is among the largest law firms in southeastern Europe and the eastern Mediterranean region. Headquartered in Limassol, Cyprus, the firm also has offices in Nicosia and Paphos in Cyprus, as well as in Russia, Belgium, Hungary, Ukraine, and the Czech Republic. The firm has the strength and depth of resources to provide international businesses and their advisers with world-class standards of quality and responsiveness. All the major independent legal rating agencies place Andreas Neocleous & Co LLC at the top of their Cyprus rankings, with Legal 500 and Chambers ranking the firm as leader in every practice area.

For more information, visit our website at www.neocleous.com.

FOR MORE INFORMATION

www.neocleous.com

www.employmentlawalliance.com

Participating ELA Member Law Firms
See page 74

About the ELA

The Employment Law Alliance (ELA) is the world's largest network of labor and employment lawyers, selected for their knowledge as well as their dedication to exceptional client service. With the power of more than 3,000 leading labor, employment, and immigration attorneys in more than 120 countries, all 50 U.S. states and every Canadian province, the ELA provides seamless and cost-effective services to multi-state and multi-national companies worldwide. ELA lawyers consistently provide efficient, effective, and timely counsel – 24 hours a day, seven days a week. International businesses benefit from the ELA's reach and deep familiarity with both the local laws and local courts, and can take advantage of a single point of contact, consolidated invoicing, and regional billing rates.

For more information, visit our website at www.employmentlawalliance.com.

500 Montgomery Street, 13th Floor
San Francisco, CA 94111

www.employmentlawalliance.com

Employee Data Privacy in Europe

Essentials for Multinational Employers

The collection, storage, and transfer of personal data is an increasing concern among both employees and employers in every region of the world. Transferring data across borders is often problematic but is especially so from countries within the European Economic Area (EEA) to the U.S.

This publication is based on a webinar presented by the Employment Law Alliance in March 2015 focusing on employee data privacy in Europe. It sets forth various privacy issues that employees and employers are likely to face in the workplace and the steps they can take to avoid, address, and resolve them.

The three key issues addressed during the webinar – and again in this publication – are:

- the transfer of employee personal data outside of the European Economic Area*;
- monitoring employees while at work; and
- posting potentially incriminating photographs and/or comments about an employer or other employees on Facebook or via other social media avenues.

For this publication, one to five questions were posed under each issue and responses were compiled from ELA members representing 24 European countries.

The responses in the following pages are grouped by country. See list at right for the countries included and the page number for each. See page 4 for the specific questions.

***IMPORTANT NOTE TO READERS:**
On October 6, 2015, the European Court of Justice issued a ruling that annulled the previous respective decision by the EU Commission (2000/520/EC dated July 26, 2000). This means that, as of this date, what is essentially the most important legal basis for the legally compliant transfer of personal data from the EU to the U.S. is not effective anymore. There are several main arguments for this ruling, but the result is that, if a transfer of data has been based on the Safe Harbor Program, companies must switch to the EU Standard Contractual Clauses, Binding Corporate Rules, or any other adequate guarantee. For more information, please contact your ELA member attorney.

COUNTRIES REPRESENTED

The Questions

Transfer of Personal Data of Employees Outside of the European Economic Area*

The responses in this section are based on the following hypothetical from the March 2015 webinar, "Employee Data Privacy in the EU: Essentials for Multinational Employers," presented by the Employment Law Alliance.

Umpire Inc., a public company established in the United States, is required by law (Sarbanes-Oxley Act) to establish an internal whistle-blowing policy, which is applicable to all of its subsidiaries regardless of location. According to the policy, whistle-blowing reports have to be filed with Umpire's Audit Committee in the U.S., thereby requiring the transfer of personal data across borders. Umpire is not Safe Harbour-certified.

- Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?
- When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?
- Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

Monitoring of Employees

- What are the relevant laws concerning monitoring of employees at work – both off- and online?
- If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?
- What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?
- Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?
- What damages/remedies do employers face in case of illegal monitoring of employees?

Use of Social Media

- Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

***IMPORTANT NOTE TO READERS:**
On October 6, 2015, the European Court of Justice issued a ruling that annulled the previous respective decision by the EU Commission (2000/520/EC dated July 26, 2000). This means that, as of this date, what is essentially the most important legal basis for the legally compliant transfer of personal data from the EU to the U.S. is not effective anymore. There are several main arguments for this ruling, but the result is that, if a transfer of data has been based on the Safe Harbor Program, companies must switch to the EU Standard Contractual Clauses, Binding Corporate Rules, or any other adequate guarantee. For more information, please contact your ELA member attorney.

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

Under the Albanian Law on Personal Data Protection and the relevant acts of the Commissioner for the Freedom of Information and Personal Data Protection (the Commissioner), personal data cross-border transactions can take place with "receivers" situated in countries with adequate levels of personal data protection. This has been held by the Commissioner to include Member States of the European Union, EEA countries, and receivers in the United States who are members of the Safe Harbour Programme.

There is, however, an exception that may allow for transfers to countries without adequate personal data protection if it can be shown that the data subject has given the requisite consent; the transfer is necessary for the performance of pre-contractual terms between the data controller and either the data subject or a third party with an interest in the data subject; there is a legal obligation to transfer; the transfer is necessary for the protection of the data subject's vital interests; the transfer occurs in virtue of instructions issued by the Commissioner; and the transfer is authorised by the Commissioner. Moreover, transfers may take place under the EU Standard Contractual Clauses and the Obligatory Corporate rules.

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

Despite the law providing for the use of the EU Standard Contractual Clauses, in practice the Commissioner requires that data controllers wishing to transfer to countries without adequate levels of protection should apply for the Commissioners' authorisation. This should be via a standard application form, with a formal request addressed to the Commissioner, and include the EU Standard Contractual Clauses and/or the Obligatory Corporate Rules. There are no set time limits for issuing the authorisation.

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

The rules outlined above are also applicable for the transfer of whistle-blowing reports (which scenario is not specifically determined by the Albanian applicable law) containing personal data within a multinational to a country outside the EEA. Nevertheless, it is recommended that the relevant subsidiary obtain the consent of its employees if personal data is to be transferred. The subsidiary could justify the process as "substantial for protecting its rights and lawful interests" in order to be fully compliant with the Law on Personal Data Protection, as well as the Albanian Labour Code.

CONTENTS

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- The Albanian Labour Code
- The Law on Personal Data Protection and its sublegal acts
- The Albanian Criminal Code

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

Generally, employers should not collect information about their employees, except where such information relates to the employee's professional skills or it is necessary for the performance of the employment contract.

Nevertheless, if misconduct or a breach of contractual duties is discovered during the unlawful monitoring of employees, any evidence gathered as a result would not affect the dismissal process to the detriment of the employer. However, there may be negative consequences if the employee raises counterclaims regarding his/her privacy/correspondence, or under the sanctions for unlawful monitoring contained in the Albanian Labour Code or the Law on Personal Data Protection.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

The applicable legislation is silent with regard to any information/consultation/co-determination rights relating to employee representatives in connection with monitoring employees. However, any kind of organization of employees, such as trade unions, may address the court regarding the protection of interests of each of its members in order to achieve compliance on the part of the employer with the provisions of the Albanian Labour Code, any applicable collective agreements, and/or individual employment contracts.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

As Albania is not a member of the EU, the upcoming changes shall not affect or apply to domestic legislation. However, Albania is in the process of adapting domestic law to be more in line with the EU acquiscommunautaire; therefore the Government is paying close attention to the harmonization of EU legislation and how EU Member States transpose this into national law.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

An employer could face both administrative and criminal sanctions for illegal monitoring, depending on the severity of the claim. Under the Albanian Labour Code, the employer may be subject to a fine of up to 30 times the applicable minimum salary, as well as possible fines under the Law on Personal Data. However, if this is a recurrence or if the breach affects several employees, the fine can be up to five times the maximum fine set for an individual breach under the Labour Code.

The criminal offences provided for by the Albanian Criminal Code stipulate that any unfair interference in one's private life, an unauthorised disclosure of personal secrets, or breaches of correspondence may be punishable by fine or imprisonment for up to two years.

The employee would also be entitled to seek damage relief from the employer before the court in cases of unlawful processing of personal data under the relevant provisions of the Albanian Civil Code.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

In cases of termination with notice, the employer is not obliged to reveal any formal cause for termination, provided the dismissal is for a reasonable cause that does not fall under the list of unjustified grounds for termination as determined by the Albanian Labour Code.

Under the Albanian Labour Code, this is considered termination for discriminatory motives and/or termination for motives related to the exercise of a constitutional right of the employee, which does not infringe on the obligations resulting from the employment contract. The employer must comply with the termination procedure and notice requirements provided for by the Labour Code.

With regard to termination with immediate effect, the employer at any time may terminate the employment contract for justifiable grounds as provided in the Labour Code. Justifiable grounds are considered to be all circumstances that, in virtue of the principle of good faith, would not allow for continuing the employment relationship, and are considered cases of serious misconduct or repeated fault, despite the employee having received written warning.

It is for the court to assess if there are justifiable grounds for the immediate termination of the employment contract. In any case, the employer should respect the termination procedure provided in the Albanian Labour Code.

Photographs of employees exhibiting inflammatory behaviour and insulting comments posted via social media, for example, would justify termination with immediate effect, as they appear to constitute breach of the principle of good faith. Nevertheless, to prevent any eventual claims by the employee regarding breach of privacy as a result of illegal monitoring, the employer should notify and obtain the consent of the employee about the monitoring actions (i.e., ensure that its social media policies comply with the applicable legislation).

For more information about transferring personal data in Albania, please contact:

Renata Leka
Boga & Associates
T: +355 4 2251 050
rleka@bogalaw.com
www.bogalaw.com

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

Under Austrian Data Protection Law, data shall be transferred only if the transfer originates from a legal data application and the interests of the data subject are not infringed by the purpose and content of the transfer.

If these conditions are fulfilled, the data controller (in this case, Umpire) then has to examine whether the transfer is subject to approval by the Austrian Data Protection Authority (ADPA). Approval is not needed where the transfer of data is to recipients in signatory states of the EEA, recipients in third countries with an adequate level of data protection, or that take place on a legal basis as stated by the law (such as the consent of the data subject). If no legal exemption applies (as is the case with the transfer to Umpire), the pre-approval of the ADPA is required. As such, the data controller has to prove an adequate level of data protection at the data recipients' location. This can be done using the EU Standard Contractual Clauses, the Corporate Binding Rules, or any other adequate guarantee.

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

According to Austrian data protection law, the EU Standard Contractual Clauses have to be approved by the ADPA, even if they are used in an unaltered version.

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

In general, local subsidiaries would have to implement a whistle-blowing scheme in accordance with Austrian data protection law. This means that a whistle-blowing scheme has to be built on a legal basis, such as overriding interests of the data controller to process data resulting from a report made of any recognised misconduct within the company. Such a report may be transferred to the parent company (Umpire) under the conditions outlined above. However, based on decisions by the ADPA, the report shall be handled at a local level in the first instance, except where the misconduct concerns management or the abuse has significant impact on the company.

CONTENTS

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- Federal Act Concerning the Protection of Personal Data (English/German)
- Works Constitution Act
- Civil Code

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

In general, no. It is at the discretion of the judge in Austrian Civil Courts as to whether the "poisoned" evidence should be considered admissible.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

Depending on the type of monitoring conducted by the company, rights of information, consultation, and co-determination may be relevant. In some cases, the law requires council consultation and approval before the employer may implement a planned measure. If the employer and the Works Council are not able to reach agreement in cases where approval is required, the employer is not allowed to introduce the measure. In other cases, the Works Council's consent may be replaced by a conciliation board that is established within the appropriate labour court, whose decision is binding on all relevant parties.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

Currently, Austrian law does not anticipate any major changes to the legal landscape with the exception of the "consent principle." This is often used to justify the monitoring of employees, provided it is not an ad hoc investigation.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

If data has been used contrary to the provisions of the Austrian Data Protection Act, the employee shall have the right to sue for damages pursuant to the general provisions of civil law, or may file for injunctive relief at the competent court. An administrative offence punishable by a fine of up to € 10,000 may also be granted against anyone who violates Austrian Data Protection Law.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

The employer has the right to terminate an employment contract that is concluded for an indefinite period of time without particular reasons by respecting the mandatory provisions on periods of notice and the effective dates of termination.

A termination without notice requires a cause that is sufficiently important to make any further employment unacceptable. Such reasons are set out on a statutory basis or, if applicable, in collective bargaining agreements.

With regard to photographs of employees exhibiting inflammatory behaviour, under the Austrian Employee Act, disloyal behaviour is a sufficient basis for termination without notice. Both the Trade Act and the Employee Act state that committing a crime is considered to be a reason for dismissal. Any photographs that depict behaviour that can be qualified as disloyal and understood to be wilful damage to property can be a justified reason for dismissal.

In relation to insulting comments posted via social media, under the relevant statutory provisions, the severe insult of the employer is also likely to be considered a justified reason to dismiss an employee with immediate effect.

In both cases the worker has no entitlement to further wage payments; however, the employer must pay the employee any remaining leave and pro rata special payments.

For more information about transferring personal data in Austria, please contact:

Hans Kristoferitsch
CHSH Cerha Hempel Spiegelfeld Hlawati
T: +43 1 514 35-191
hans.kristoferitsch@chsh.com
www.chsh.com

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

Under Belgian law, the transfer of personal data to a third country outside the EU is authorised only if the country of destination can ensure an adequate level of protection. If this is the case, the transfer can take place as if it were a transfer within the EU. However, the general principles of the Belgian Data Protection Act (DPA) must be observed.

If the level of protection is considered to be inadequate, a transfer may still be allowed in limited cases. This means that companies must, in general, formalise a transfer of personal data through any of the following methods: drafting a contract based on the EC Standard Contractual Clauses for the transfer of personal data to third countries; drafting Binding Corporate Rules, which are then authorised by Royal Decree after approval from the Belgian Privacy Commission (BPC); or, in specific and exceptional cases, relying on one of the exceptions (such as the consent of the data subject). Until recently, transfer of data to the U.S. was allowed by subscription to the Safe Harbour Principles. The CJEU's court decision of October 6, 2015 has declared the Safe Harbour rules invalid. Companies cannot, therefore, rely anymore on the Safe Harbour rules for transferring data to the U.S., but should rely on one of the alternative methods.

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

No such national authorisation is required. However, the company must send a copy of the contract to the BPC and register in the BPC public register, subject to exceptions.

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

Whistle-blowing in the private sector is not regulated in Belgium. The BPC has issued a Recommendation stating that whistle-blowing systems must be privacy-proof and comply with the DPA. Employers are advised to follow this Recommendation when setting up a whistle-blowing system.

The obligation for the parent company to comply with the Sarbanes-Oxley Act is not, as such, a sufficient legal obligation for the local subsidiary to process or transfer whistle-blowing reports. However, compliance with Sarbanes-Oxley and the risks related to non-compliance will be taken into account in judging whether the local subsidiary has a legitimate purpose for processing and transferring the reports.

The BPC recommends that whistle-blowing reports should be made only where no solution is found through the normal hierarchical system at work. The Recommendation does not state what kind of irregularities can be disclosed, as long as they are seriously substantial and relevant. However, the whistle-blowing system must be proportionate, and anonymous reports are discouraged.

CONTENTS

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- Data Protection Act 1992 (ensuring privacy protection against wrongful processing of personal data)
- Collective Bargaining Agreement n° 81 (ensuring employees' privacy protection in case of cyber surveillance, control on electronic online communication data)
- Collective Bargaining Agreement n° 68 (ensuring employees' privacy protection in case of camera surveillance)
- Collective Bargaining Agreement n° 9 and n° 39 (regulating information and consultation of consultative bodies: note that consultative bodies only have to be informed and/or consulted in certain cases, but never have a determination right)

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

In cases where evidence is gathered in an unlawful way, it is for the Court to decide whether or not to admit that evidence. The Court will use its discretion to examine the facts of the case as a whole, the way in which the evidence was obtained, and the circumstances under which the unlawful act was committed. If a case involves the wrongdoing of an employee that is sufficiently severe, it is more likely that the Court will rule the breach of privacy legislation is justified.

Prior decisions have accepted that the court can admit unlawfully obtained evidence insofar as the compliance of the provision being repudiated is not prescribed under penalty of nullity, and the unlawful gathering of evidence does not undermine the reliability of the evidence or jeopardise the right of a fair trial.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

Consultative bodies have an information and/or consultation right in certain cases, but they never have a (co-)determination right.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

The upcoming changes in EU regulation shall not, in principle, change the monitoring of the employees through collective bargaining agreements.

However, as sanctions are increasing and national supervision is more strictly organised, the upcoming EU regulation shall have an impact on all employees' privacy infringements. The consent principle in employment is already debated in Belgium because of the employee's subordinate position toward the employer. This means that employers cannot rely on consent only to legalise monitoring employees.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

Apart from the admissibility of evidence risk, non-compliance with data protection or monitoring legislation entails criminal penalties.

Employees who are victims of privacy violations may also claim compensation and damages or file a complaint with the BPC.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

In general, employees are allowed to express critical comments regarding their employer, as long as there is a balance between the freedom of speech and the employee's obligation of loyalty.

However, case law in Belgium has accepted that the misuse of social media (e.g., Facebook/Twitter) is a severe cause/urgent reason for terminating the contract without notice or compensation/severance.

In general, the concrete circumstances will be the deciding factor for a judge as to whether there is a severe cause/urgent reason for termination. This would include whether or not the employer has a social media policy, if the employee had received any previous warnings, the identity and function of the employee misusing social media, and if the employee intended to harm the company. Employers are therefore strongly encouraged to implement a social media policy with clear instructions on what is and is not acceptable.

For more information about transferring personal data in Belgium, please contact:

Jan Hofkens
Lydian
T: +32 (2) 787 90 37
jan.hofkens@lydian.be
www.lydian.be

Isabel Plets
Lydian
T: +32 (2) 787 90 83
isabel.plets@lydian.be
www.lydian.be

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

The general rule under Bulgarian law is that, for each transfer to a country outside the EEA, the transferring company (i.e., transferor) should ensure an adequate level of protection for the personal data being transferred and request the Bulgarian Commission for Personal Data Protection (CPDP) for permission or confirmation of the exact transfer.

The transferor may then proceed with one of two options:

1. The transferor and the transferee conclude the EU Standard Contractual Clauses with regard to the transfer without any material changes. The EU Standard Contractual Clauses represent clauses for the transfer of personal data to processors established in third countries, as provided by Directive 95/46/EC of the European Parliament and of the Council, approved by a decision of the European Commission.

In this case, the authority verifies only that the EU Standard Contractual Clauses are not significantly changed and are being used properly before confirming the transfer's lawfulness. Thus, the procedure before the CPDP is simply a confirmation.

2. The transferor and the transferee conclude an ad hoc agreement different from the EU Standard Contractual Clauses, which affirms that the parties have ensured an adequate level of protection of the personal data subject to the transfer.

In this case the CPDP conducts a permission procedure consisting of: (i) a revision and analysis of the conducted agreement; (ii) adoption of an explicit decision whether the used clauses provide the necessary level of protection; and (iii) issuance of a permit or rejection of the revised transfer.

For transfers of personal data, the Bulgarian CPDP also requires the transferor to notify the affected individuals in advance and separately for each transfer. The notification should contain all information concerning the transfer, such as:

- the exact data that will be subject to the transfer;
- the ground/s and the aim of the transfer;
- the receiving party;
- how long the transferee will keep the transferred data;
- how the concerned individuals can request access and amendments to their data.

Each change in the parameters of a transfer is considered a new transfer and the above procedures for CPDP permission and notification to the concerned individuals are to be commenced and completed by the transferor.

CONTENTS

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

Yes. The transferor is required to initiate and comply with a formal confirmation procedure by presenting the executed EU Standard Contractual Clauses to the CPDP for the transfer. This procedure is less complicated than when the transfer is not based on these clauses. In this instance, the commission only needs to verify that: (i) there are no material changes in the used EU Standard Contractual Clauses, and (ii) the revised contractual relation does not contradict either the provision for an adequate level of protection or the requirements of the EU Standard Contractual Clauses.

An additional authorization (permission) will be needed in instances where there is a transfer of sensitive personal data (e.g., data on the medical status of the employees, participation in trade unions, etc.). As such, the transferor should indicate in its batch with the Register of Personal Data Controllers held by the CPDP that it processes sensitive personal data and possesses the needed authorization to do so. And, as above, the transferor should obtain in advance the explicit consent of the concerned individual.

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

Bulgarian law does not provide for any explicit regulation regarding the transfer of whistle-blowing reports containing personal data.

Regardless, the involved employer should follow the main principles for personal data processing and transfer provided by the Bulgarian and applicable EU legislation. It also should provide maximum protection of the employees' rights, including:

- the whistle-blower's scheme, to be introduced to the employees through the employer's internal rules. As a result, the data collection will be grounded and have legitimate aim;
- notifying the affected employee as soon as possible with details on the specific data processing and his/her rights;
- complying with the main principles of Bulgarian and EU personal data protection legislation – e.g., providing access to the personal data. See Opinion 1/2006 adopted by the Article 29 Data Protection Working Party with regard to the processing of personal data.

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- Constitution of the Republic of Bulgaria
- Personal Data Protection Act
- Bulgaria Labour Code and the related subordinate legislation

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

In general, no. However, illegally acquired evidence is not accepted by the court. If an employee proves damages occurred as a result of illegal monitoring, he/she is entitled to claim remedy.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

Employment law compliance: The employer should inform the employees' representatives in advance about any changes in its enterprise that are related to or may affect the employment relationship. This includes the implementation of any type of monitoring. The representatives' consent is not necessary, but they should have an opportunity and enough time to give their opinion, comments, recommendations, etc.

Personal data protection compliance: If the monitoring of employees includes personal data processing, prior to implementation the employer should provide specific information on the chosen type of monitoring, including: the purpose and type of monitoring, why it is necessary, how the data will be collected and kept, how long the data will be kept, how the data might be used, who will be granted access to it, etc.

If the monitoring applies to the processing of personal data that requires the consent of the concerned individuals, the employer should obtain the employees' consent in advance. However, the Bulgarian Personal Data Protection Commission presumes that, due to the subordination and the lack of choice on the part of the employees, their consent is questionable and should not be the only ground for the monitoring.

As a general comment to the above, due to the lack of specific regulations regarding employee monitoring, it is advisable, prior to the implementation of any type of monitoring, for an employer to make a full assessment of all required compliance and potential risks.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

It is expected the current regulation procedures will be a relief.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

The monetary sanctions for non-compliance with the personal data protection requirements are up to € 50,000.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

The employer should view incriminating and/or insulting posts and uploads to Facebook very carefully in light of the personal rights of employees (e.g., freedom of speech) coupled with any written employment rules and regulations (e.g., whether the company has a social media policy). Furthermore, any use of an employee's illegally obtained personal data may not be ground for termination of the employment contract.

Each case should be considered separately, depending on the specific circumstances, such as the employee's job position (e.g., whether he/she is a publicly recognized and followed person); the damages incurred; whether more important rights, for example, of entire society groups are concerned by the post, etc.

As a general rule, due to the limited causes for termination provided by Bulgarian law, the employer will need to further investigate the situation and, if it decides to use the posts/uploads to social media as a basis for termination, the posts should be only part of the facts supporting the cause for termination.

The disciplinary liability of the employees for posts in social media depends on:

- the availability of their posts;
- the specifics of the employment function and relation;
- the internal rules of the employer;
- who is the protected interest.

Based on this, the employer should assess whether the specific posts/uploads and any other collected information and evidence on the case are sufficient enough to sustain a termination cause listed by the law (e.g., dismissal due to an abuse of the employer's confidence). If yes, the employer should further follow the specific procedure for termination depending on the chosen cause, as required by law.

For more information about transferring personal data in Bulgaria, please contact:

Vesela Kabatliyska
Dinova Rusev & Partners Law Office
T: +359 (0)2 903 01 01
vesela.kabatliyska@drp-legal.com
www.drp-legal.com

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

Personal data contained in personal data filing systems may be transferred abroad from the Republic of Croatia for further processing only if the receiving country or international organization can ensure an adequate level of protection. In case of reasonable doubt, prior to transferring personal data abroad, the filing system controller shall obtain an opinion from the Personal Data Protection Agency (the AZOP).

Until recently, under certain circumstances, U.S.-based companies (organisations) were deemed to provide an adequate level of protection (e.g., compliance with the Safe Harbour Principles). However, after the Court of Justice invalidated the Safe Harbour framework of 2000 reached between the U.S. and the European Commission and declared the Commission's Decision 2000/520 to be invalid as of 26 July 2000, the AZOP considers the U.S. not to provide a sufficient level of protection of personal data.

If the receiving country does not provide for an adequate level of protection, the transfer of personal data shall only be allowed if one or more of the exceptions prescribed in the Croatian Personal Data Protection Act are met. These include: the employee's consent for disclosure of the personal data (but only for the purpose for which the consent was given); the employer's guarantee for the protection of privacy and fundamental rights and freedoms of the employee; when the transfer of personal data is necessary for the performance of a contract between the employee and the employer, or for the implementation of pre-contractual measures taken in response to the employee's request; or the transfer of personal data is necessary for the conclusion or performance of a contract between the employer and a third party that is in the interest of the employee.

CONTENTS

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

Transfer of personal data to a country that does not provide an adequate level of protection is allowed when the AZOP decides that the conditions for such a transfer are based on or in line with the Standard Contractual Clauses adopted by the European Commission. The transfer of personal data can be effected only after a Croatian subsidiary provides the AZOP with the respective agreement concluded with a company and upon the AZOP's decision determining that the agreement provides a sufficient level of protection.

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

Transfer of whistle-blowing reports containing personal data as such is not particularly regulated in the Croatian law. Such transfer shall instead be subject to the general rules that apply to the transfer of personal data.

Generally, the Croatian subsidiary needs a justification for the processing and transfer of personal data to a parent company, whereas an obligation of the parent company to establish a whistle-blowing scheme shall not automatically be deemed a justified reason for transferring personal data under the Croatian laws. If the parent company does not have the employees' consent for the transfer of personal data, but the Croatian company does have a legitimate interest for the transfer within the whistle-blowing scheme (or the parent company as a third party), the processing of personal data shall be allowed unless the fundamental rights and interests of data subjects are greater than the company's (or parent company's) legitimate interest. That is to say, the mere existence of certain legal obligations on the part of the parent company under the Sarbanes-Oxley Act shall not automatically mean legitimate interest of the Croatian subsidiary to processing and transferring personal data within the whistle-blowing scheme.

Prior to collecting any personal data, the Croatian subsidiary shall inform the employees whose personal data are being collected of the identity of the personal data filing system controller, the purpose of the processing, right to access of data, personal data users or personal data user categories, and whether such data provision is voluntary or mandatory, as well as the possible consequences for withholding the data.

Prior to creating a personal data filing system, the Croatian subsidiary shall notify the AZOP of its plans to create such a system, including any plans to further process data, whereas the Croatian subsidiary shall create and maintain records on respective personal data that are to be collected, processed, and transferred to the parent company, and delivered to the AZOP within 15 days at the latest of its creation.

Pursuant to the Employment Act, the Croatian subsidiary needs to obtain approval by the workers council prior to adopting the decision on the collection, processing, use, and transfer of the employees' personal data to the parent company. The Croatian subsidiary shall define in the employment by-laws the data on the employees that it will collect, process, or transfer to the parent company as a third party.

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- Constitution of the Republic of Croatia
- Personal Data Protection Act Employment Act
- Obligations Code
- Criminal Code
- Legal Persons Criminal Liability Act

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

If the evidence of misconduct is gathered illegally (e.g., without an employee's consent in favour of monitoring), the evidence cannot have a binding effect on the court.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

Information, consultation, and co-determination can be relevant.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

It is still not known, but the general belief is "no." Croatia, as a new EU member state, has a detailed legal framework of data privacy/data protection laws.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

Illegal monitoring (i.e., unauthorized collection and processing of personal data), as well as unauthorized recording, represent a criminal act. In addition to criminal liability, under civil law, employees could sue the Croatian subsidiary for a court order to cease and desist from such measures and claim compensation for damages. Furthermore, the Croatian subsidiary, as the employer, can be faced with a misdemeanour fine up to € 7,500.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

The justified reasons for termination (ordinary/extraordinary) are not prescribed by the law, but shall be decided by the court, taking into account the particular circumstances of each case. Even though Croatia has not implemented a system of precedents, court practice plays a significant role in assessing whether an employee's act or ommision may be considered as a justified reason for either ordinary or extraordinary termination. For employees who post disparaging or offensive photographs on Facebook or other social media, extraordinary termination is not only justified but also inevitable to protect the reputation of the employer. In such cases not only is the employee not entitled to severance pay, but the employer may be entitled to compensation of damages should its reputation be jeopardized as a result of the employee's action.

Likewise, there is no straightforward response to an employee who posts incriminating or insulting comments on Facebook about the company and/or other employees, including whether such statements are sufficient for immediate termination of employment. Each case needs to be analyzed on its merits, taking into account whether the comments were made public, etc. In general, it is easier to terminate employment by giving an ordinary dismissal, in which case a prior written notice shall be handed over to the employee, than by giving extraordinary notice. In none of the cases, however, would an employee be entitled to severance pay.

For more information about transferring personal data in Croatia, please contact:

Hrvoje Vidan
Vidan Law Office
T: +385 1 4854 070
hrvoje.vidan@vidan-law.hr
www.vidan-law.hr

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

The transfer of personal data to third countries outside the EU is allowed only if the relevant license has been issued by the Commissioner for the Protection of Personal Data (the Commissioner). The Commissioner will not issue such a licence unless it is satisfied that the country can ensure a satisfactory level of protection, based on a number of criteria, including: the nature of the information; the purpose and duration of the processing; the general and special rules of law; and if the relevant fees have been paid. Prior to the Schrems ruling, the transfer of data to the U.S. was allowed if the company to which the data would be transferred participated in the Safe Harbour system. After the Schrems ruling in October 2015, and until this matter is clarified at the EU level and the Commissioner takes an official position, authorisation from the Commissioner should be obtained and using Binding Corporate Rules and Standard Contractual Clauses is advisable for the transmission of personal data to the U.S., even where the recipient of the data in the U.S. is Safe Harbour certified. The outcome of the relevant Article 29 Working Party's assessment on this matter will be forthcoming soon.

The transfer of personal data to a country that does not ensure an adequate level of protection may be allowed under the law if the employer can guarantee the protection of the personal life and fundamental rights of the employees involved, or where it can be shown that one or more of the specific statutory conditions shall apply. These include: if the employee has given consent freely to the transfer; the transfer is necessary for the performance or entering into of (pre-)contractual terms between the employer and the employee; the transfer is necessary to secure a vital interest of the employee; etc.

CONTENTS

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

The Standard Contractual Clauses that have been approved by the European Commission may be considered as providing satisfactory guarantees for the purposes of the law. However, the contracts and clauses must be submitted to the Commissioner for approval so that a license is issued before any intended international transfer of personal data takes place.

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

The conditions regarding the transfer of personal data of employees are mentioned above.

It would be difficult under the law to justify that such processing would be necessary for complying with a legal obligation. The processing in these circumstances, therefore, must be justified as necessary for the legitimate interest of the company, and the fundamental rights and interests of the data subject should not outweigh the company's interest. Thus the principles of proportionality and subsidiarity, the seriousness of the alleged offences, and the consequences for the data subjects shall need to be taken into account, as well as any adequate safeguards that are in place for protecting the personal data.

Under normal circumstances, reports on improper conduct of any nature should be handled through the regular channels, such as the management hierarchy, human resources, or the employee representatives. The use of any whistle-blowing scheme must comply with the requirements of the law and the relevant principles of data protection. It cannot replace regular reporting systems, and its purpose needs to be limited to very serious misconduct.

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- The Processing of Personal Data (Protection of the Individual) Law of 2001
- The Protection of the Privacy of Personal Communications (Monitoring of Conversations) Law of 1996

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

Following numerous decisions by the Supreme Court in Cyprus, any evidence obtained in breach of a person's right to respect of private life and confidential communication, which is protected under the Cyprus constitution, is inadmissible.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

Employers must notify their employees in advance about the purpose, method, and duration of the control and monitoring that they intend to apply. Consultation is not required by law, but employers wishing to install monitoring systems at the workplace are encouraged by the Commissioner to consult employees or their trade union or other representatives to discuss the intended methods and consequences of monitoring.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

In general, the upcoming changes to EU regulation shall not change the legal landscape in Cyprus with regard to data privacy or data protection of employees.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

Under the law, the Regulator has the authority to issue warnings, impose fines, revoke licenses (either temporarily or permanently), or order the cessation or destruction of the relevant data. Compensation by way of general damages may also be ordered by the Court, depending on the seriousness and consequences of the offence.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

The voice, picture, email address, and phone number of employees are considered personal data. If collected through monitoring systems installed by an employer in the workplace, they may be used only for the purposes for which they are intended, and then destroyed/deleted after these purposes have been accomplished.

Before an employer installs a monitoring system, it must first examine whether the intended control and monitoring, as well as the data to be collected, are proportionate to the purpose it seeks to accomplish. It is not always necessary to monitor all employees or all of their activities and communications. The employer must chose the lowest level of monitoring that is sufficient to satisfy his purposes, with the aim of as little intrusion as possible to the personal life of employees. Secret monitoring or monitoring without previous notice is prohibited in any event.

Regardless, serious misconduct such as posting pictures of employees disparaging the employer or the employer's image would normally justify immediate termination of employment without notice and compensation. However, the employer would not be able to rely on evidence obtained if the monitoring is carried out in violation of the above requirements.

In relation to posting derogatory comments about the employer or other employees on social media, under Cyprus law there is no express duty of loyalty that limits an employee's use of social media, although employees owe a general implied duty of fidelity to their employers that includes refraining from any actions that are inconsistent with this obligation (either on- or offline) and obeying reasonable instructions of the employer, including legitimate company policies. Applying a social media policy with clear guidelines is advisable and may prevent unacceptable behaviour. It should be noted that monitoring an employee's social media must also comply with the requirements of the law for monitoring.

Under the circumstances above, it may be advisable to warn the employee not to repeat any insulting or derogatory statements rather than terminate his/her employment right away, as this may give rise to an action for unlawful dismissal. Such misconduct arguably may not be considered serious enough to justify immediate termination of employment; however, every case will need to be considered based on its own facts.

For more information about transferring personal data in Cyprus, please contact:

Nicholas Ktenas
Andreas Neocleous & Co LLC
T: +357 22 110324
ktenasn@neocleous.com
www.neocleous.com

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

Under Czech law, personal data can be transferred outside the EEA if:

- Free movement of personal data, i.e., a ban on restricting movement of such data, ensues from an international treaty to which the Czech Parliament has given its consent, and that binds the Czech Republic (this relates especially to countries that signed the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, No. 108, 1981); or
- Personal data are transferred on the basis of a decision of an institution of the European Union, e.g., Commission Decision No. 2010/87/EU as of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries. Note that Commission Decision no. 2000/520/EC as of 26 July 2000 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the U.S. Department of Commerce, was recently (October 2015) declared invalid by the Court of Justice of the European Union and, therefore, it is no longer possible to transfer personal data in accordance with this Decision).

If neither of the above conditions is met, personal data may be transferred if the controller proves certain facts (e.g., the data transfer is carried out with the consent of the data subject, sufficient specific guarantees for personal data protection have been created in a third country, etc.) to the Czech Data Protection Authority (DPA) and the transfer is authorized by the DPA in special proceedings.

Thus, in the example provided, Umpire Inc. may transfer personal data under the EU Standard Contractual Clauses or after the DPA grants its authorization.

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

No authorization is required if the EU Standard Contractual Clauses (unmodified) are used. In this case, the condition for free movement of personal data in accordance with Section 27 of Personal Data Protection Act is fulfilled. The concluded Clauses are usually attached to the personal data processing notification to the DPA, or the DPA may request them according to Section 16 (4) of Personal Data Protection Act.

If the Standard Contractual Clauses are modified (i.e., if they do not correspond to the wording of the relevant Commission Decision), the authorization of the DPA will be required. When considering the application for the authorization, the DPA examines (in accordance with Section 27 (4) of Personal Data Protection Act) all circumstances related to the personal data transfer with regard to available information about legal or other regulations governing the personal data processing in the third country. In particular, the DPA examines the source, the final destination and categories of personal data that are to be transferred, and the purpose and period of the processing.

CONTENTS

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

There is no special regulation of whistle-blowing (reports) in the Czech Republic. However, once the report contains personal data, it is necessary to proceed in accordance with the Personal Data Protection Act, including its principles. As such, the data may only be processed in accordance with the purpose for which they were collected and for a period of time that is necessary for the purpose of their processing; the data controller must comply with certain information obligations vis-a-vis the data subjects; and it is necessary to notify the DPA on personal data processing or perform data transfer in accordance with the law as described above.

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- Act No. 262/2006 Coll., the Labour Code
- Act No. 101/2000 Coll., the Personal Data Protection Act
- Constitutional Act No. 2/1993 Coll., the Charter of Fundamental Rights and Basic Freedoms
- Act No. 40/2009 Coll., the Criminal Code

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

Under certain circumstances illegally gathered evidence may be presented. Under Czech case law, it is necessary to assess the illegality/usability of evidence on a case-to-case basis, especially with regard to the nature of the breach, the influence of the particular evidence, and the relevance of such evidence for the proceedings.

Employee status is strengthened by law and monitoring of employees is possible only under (strict) conditions set by law. Therefore, evidence gathered illegally by monitoring of employees will be inadmissible.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

Generally, the employer has certain information and consultation obligations vis-a-vis its employees, including the obligation to inform employees of and consult with them about the basic aspects of the working conditions and any changes thereof (including the implementation and operation of the monitoring system). These obligations may be fulfilled through employee councils or trade unions if they exist within the employer. However, neither employee representatives nor employees themselves have the right to be involved in the co-determination procedure.

Moreover, the employer is also obliged to inform its employees about any monitoring system in accordance with the conditions set out in the Labour Code and Personal Data Protection Act.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

No, the upcoming EU data protection regulation should not have any direct impact regarding employee monitoring, as this is a labour-law issue, which should not be directly affected by the new data protection legislation.

There may, however, be certain indirect changes. For example, the new penalties may require employers to exert greater efforts to comply with their obligations under the data protection legislation.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

Employers face the following types of damages/remedies for illegally monitoring employees: the DPA may impose cash penalties for personal data processing that fails to comply with the Personal Data Protection Act in accordance with Sections 44 et seq.; the relevant Labour Inspectorate may, according to the relevant provisions of Act No. 251/2005 Coll., the Labour Inspection Act, impose cash penalties for failure to comply with the Labour Code and other related legal regulations; and employees may claim damages for breach of their privacy according to the Act No. 89/2012 Coll., the Civil Code. Serious cases of illegal monitoring are subject to criminal prosecution and penalties according to the Criminal Code.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

The Czech Labour Code stipulates that employees may not use the employer's means of production and working means, including computers, for their personal needs. The employer may check any time whether or not employees are complying with this obligation.

Employers may dismiss an employee immediately for a gross breach of duty arising out of the legal regulations applicable to the work performed by the employee.

An employee may also be dismissed due to repeated, less serious breaches of a duty arising out of the legal regulations applicable to the work performed by the employee if he/she has been advised in writing of the possibility of dismissal within the last six months.

With regard to uploading or posting incriminating and/or insulting photos or comments on Facebook, it will be necessary to assess on a case-to-case basis whether the employee's conduct gives rise to some of the grounds for dismissal, i.e., if the employee breached his/her duties in an especially gross manner or committed a gross or repeated less serious breach of his/her duties. Using social media during working hours may be regarded as a breach of loyalty or of working duties and therefore sufficient reason for dismissal.

For more information about transferring personal data in the Czech Republic, please contact:

Drahomir Tomasuk
Kocian Solc Balastik
T: +420 224 103 311
dtomasuk@ksb.cz
www.ksb.cz

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

The transfer of personal data from a Danish subsidiary to (in this case) Umpire requires a legal basis under the Danish Data Protection Act. The relevant legal basis for the transfer could be the conclusion of EU Standard Contractual Clauses or an ad hoc agreement between the parties where the Danish entity provides adequate safeguards with respect to the protection of rights of the data subject. Furthermore, the actual disclosure of personal data from one data controller (i.e., the Danish subsidiary) to another data controller (i.e., the parent company) also requires a legal basis, e.g. the processing is necessary for the establishment, exercise, or defence of legal claims.

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

For the transfer of personal data, if the EU Standard Contractual Clauses are used without any material changes, authorisation is unnecessary. However, if ad hoc agreements or amended EU Standard Contractual Clauses are used, the Data Protection Authority (DPA) must authorise the transfer, and the agreement must be filed with the DPA.

Authorisation is also needed to process sensitive or semi-sensitive personal data. The latter is a special Danish category, and covers personal data about criminal offences, serious social problems, and other purely private matters than those covered by sensitive personal data.

The DPA has standardised the handling of applications regarding whistle-blowing hotlines and has produced a standard form. If this is used, the DPA may handle the application within one month. If the application deviates from this standard form, it may be handled within six-12 months.

Finally, a Danish subsidiary must also obtain an authorisation to process sensitive personal data within HR-administration, i.e., the outcome of an internal investigation concerning an employee initiated by the whistle-blowing report. The DPA has also standardised the application form for HR-administration.

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

Both the transfer and the disclosure of personal data require a legal basis. This is mentioned above.

The DPA has taken the view that an entity within a multinational group may be the data controller of personal data processed within a whistle-blowing hotline. This includes non-EEA entities. In general, a legal obligation to disclose personal data would constitute a legal basis; however, the DPA does not recognise a non-EEA legal obligation.

Instead, the relevant entity may process and disclose whistle-blowing reports containing sensitive personal data if the entity or the recipient has a legitimate interest, and this interest clearly overrides the interests of the data subject in not having the personal data processed or disclosed. This also means that the reporting may take place only in cases of serious offences (or suspicion of serious offences) that can be of importance to the group/entity as a whole, or that can be of significant importance to the life and well-being of individuals.

CONTENTS

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- The Penal Code
- Data Protection Act
- Video Surveillance Act
- DA and LO's agreement on control measures (if agreed upon)

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

In general, no. However, the employee may be entitled to compensation for the illegal action even if the court holds that the employee is in fact in breach of his/her contractual duties.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

The employer will have to inform the local Works Council at a time early enough so that opinions, ideas, and suggestions from the employees can enter into the company's basis for the decision to implement measures to monitor the employees. If the employer is covered by DA and LO's agreement on control measures, it has to inform the Works Council at least six weeks before implementing the control measure and the measures can only take effect after this period. However, the measures can be implemented before notifying the Works Council if the purpose of the control measure is lost by doing so or in case of compelling operational considerations.

Further, the employer is free to implement measures to monitor employees without the consent from employee representatives as long as the measures are objectively justified by operational considerations and have reasonable purpose, they are not offensive to the employees, and the measures do not cause the employees any loss or impose any significant burdens. If the employees do not find that these conditions have been met, they can submit the disagreement to industrial arbitration.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

Generally, no. However, more severe fines may be anticipated for breach of the employees' privacy. Currently, the highest fine handed down for breach of the Danish Data Protection Act is DKK 25,000 (approx. € 3,350)

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

The violation may lead to compensation for injury to the employee's privacy.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

During the employment relationship, the employee is bound by a general obligation of loyalty towards the employer. Thus, although employees enjoy the freedom of expression, they are not free to express critical or negative comments about their employer or cause damage to their employer in any other way.

The employer's options depend on the severity of the comments or photographs, who and how many people have been able to see the comments or photographs, and the employee's position in the company. It will be considered less severe if the comments or photographs are posted to a closed forum of friends rather than to a public profile or group, or to the company's clients or customers.

Comments or photographs as a reason for termination or summary dismissal are also more likely to be accepted as just cause if the employee has received a prior warning. Likewise, it is advisable for the employer to have a clear social media policy with guidelines that stipulate possible consequences for breach of the guidelines.

In cases of unfair termination or unfair summary dismissal, the employee will be entitled to severance payment of one to three months' salary, depending on the concrete circumstances.

For more information about transferring personal data in Denmark, please contact:

Michael Hopp
Plesner
T: +45 36 94 13 06
mho@plesner.com
www.plesner.com

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

The applicable legal bases for data transfer in this case under the Finnish Personal Data Act are an agreement between the Finnish entity and Umpire implementing the EU Standard Contractual Clauses or an ad hoc agreement between the same parties, where Umpire guarantees adequate safeguards regarding the data subject's rights and processing of personal data.

The Finnish Data Protection Ombudsman must be notified of ad hoc agreements.

It is worth noting that, on 6 October 2015, the Court of Justice of the European Union ruled that the Safe Harbour agreement between EU and the U.S., which allowed the transfer of European citizens' data to the U.S., is no longer valid. The repercussion of the ruling means that any personal data transfers from the EEA to the U.S. purely on the basis of Safe Harbour regime are no longer compliant with requirements of the European Data Protection Directive 95/46/EC and, consequently, the Finnish Personal Data. However, the Court's ruling has no effect on any other legal means of transfer of personal data outside of the EEA. Therefore, the EU Standard Contractual Clauses and the above elaborate ad hoc agreements are valid under the Finnish Personal Data Act as they were prior to the Court's ruling.

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

If the EU Standard Contractual Clauses are implemented without amendments or modifications, no authorization is required. If the Clauses are amended, the agreement is considered an ad hoc agreement, and the obligation to notify the Finnish Data Protection Ombudsman described above applies.

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

The same conditions that apply to the transfer of personal data described above are also applicable to the transfer of whistle-blowing reports.

CONTENTS

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- Finnish Personal Data Act
- Information Society Code
- Act on Protection of Privacy in Working Life

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

In Finland, there are general legal principles, referred to as the principle of free production of evidence and the principle of free evaluation of evidence, which pertain to the use of illegally obtained evidence.

The prevailing rule is that courts have discretion to determine the admissibility of evidence. If data obtained through illegal means is presented in court as evidence, the court evaluates the proof value of such evidence and the extent to which, if any, it shall be taken into account in the determination of the facts in the case at hand. Evidence obtained through illegal means should be considered inadmissible for weighty reasons, such as the severity of the infringement.

Regardless of whether or not illegally obtained data is accepted as evidence, the party presenting such data should be aware that showing evidence obtained in an unlawful manner exposes itself to possible liability for that unlawful conduct.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

A company with more than 30 employees that is implementing camera surveillance or other monitoring by technical means, as well as processing personal data related to the employees' emails or other information networks, is subject to co-operation discussion procedures between the employer and employees as set forth in the Act on Co-operation within Undertakings. If a company has fewer than 30 employees, the employees or their representative still need to be informed about the essentials of the monitoring, but in a less formal manner than the regulatory co-operation discussions.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

At the present time there are no perceived and/or predicted changes to establishing and maintaining the practice of monitoring employees. However, sanctions resulting from violations of the regulatory requirements are subject to change by virtue of the administrative sanctions introduced by the new EU regulation – that is, to the extent the monitoring practices would be seen as violating the new EU regulation.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

An employer may be sentenced to a fine pursuant to the data protection laws or the Finnish Criminal Code, depending on the seriousness of the offense. In extreme cases, imprisonment is also possible. In addition, the employees in question may claim damages for breach of their privacy.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

In Finland, there are no laws or regulations specifically addressing employees' use of social media. Instead, Finnish legislation provides general principles that shall be taken into account when considering employees' use of social media. Inappropriate action occurring through social media shall be handled in the same way as any inappropriate actions that take place face-to-face.

Significantly, an employee's duty of loyalty as set forth in the Employment Contracts Act restricts the employee's behaviour and also his/her use of social media, even for private purposes and outside of working hours. The duty of loyalty requires that, in all their activities, employees shall avoid everything that conflicts with actions reasonably required of employees in their position. It is important to note that an employee's duty of loyalty also restricts his/her freedom of speech, as provided for in the Constitution of Finland. Because employees are bound by the duty of loyalty even outside of working hours, they also must not cause harm to the employer while exercising their freedom of speech regardless of time or place. Depending on the employee's position, insulting or criticizing the employer in social media may constitute grounds for dismissal.

Breach of the duty of loyalty, such as inappropriate behaviour at the workplace and/or publishing photos of inappropriate behaviour at the workplace, or insulting or criticizing the employer in social media may constitute grounds for dismissal. However, dismissal on such grounds usually requires prior warning to the employee. Only if the inappropriate behaviour is of such severity that the employer cannot reasonably be expected to continue the employment relationship is a prior warning to the employee not necessary.

Finally, systematic monitoring of the content of an employee's social media usage is not permitted in Finland without the employee's consent. While content published on social media is public and not considered confidential, in most cases, the employer still may not monitor the employee's postings, for example, on Facebook. However if a colleague prints an insulting or incriminating posting on Facebook, the employer is entitled to take necessary action and use that information in making its determination regarding possible termination. In such instances the employee should be given a chance to explain or respond before the employer makes any decisions regarding the employment relationship.

For more information about transferring personal data in Finland, please contact:

Anu Waaralinna
Castrén and Snelling
T: +358 (0) 20 7765 372
anu.waaralinna@castren.fi
www.castren.fi

Sanna Alku
Castrén and Snelling
T: +358 (0) 20 7765 392
sanna.alku@castren.fi
www.castren.fi

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

Under French Labour law, the transfer of personal data outside EEA is lawful where the outside country offers an adequate and equivalent level of personal data protection. The French Data Protection Commission (CNIL) considers that the U.S. does not provide an adequate level of protection.

Until now and for almost 15 years, the exception to this rule was the Safe Harbour Program, i.e., the European commission considered that personal data was adequately protected by U.S. companies that adhered to the Safe Harbour Program and that such data could be transferred to these companies from Europe (EC Decision of July 26, 2000).

However, the European Court of Justice invalidated this Safe Harbor Decision on October 6, 2015, as it contravenes fundamental rights and freedoms of EU citizens as provided for in EU laws and treaties. Consequently, any transfers of personal data that take place under Safe Harbor are now unlawful.

The alternatives to the Safe Harbour Program are the Binding Corporate Rules that define the terms of transfer of personal data and the EU Standard Contractual Clauses.

Pending the adoption of a sustainable and compliant solution replacing the Safe Harbour Program, the EU data protection regulators have recently confirmed that these alternatives should be implemented by U.S. companies as a basis for the transfer of personal data from the EU to the U.S.

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

When using the EU Standard Contractual Clauses, the formalities needed to gain authorisation from the CNIL depend on the purpose of the data processing. There are three main types of formalities: declaration, authorisation, or request for opinion.

With regard to the whistle-blowing policy, if the scope of the policy covers only specific areas that have already been approved by the CNIL, the policy and the transfer of personal data will be subject to a specific statement and not an express authorisation. Otherwise, if the scope of the policy is broader, the company will need an express authorisation from the CNIL.

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

The same rules apply to the transfer of whistle-blowing reports containing personal data. A Deliberation of the CNIL regarding whistle-blowing policies refers to the rules explained above regarding the EU Standard Contractual Clauses and Binding Corporate Rules (since the Safe Harbour Program no longer allows for the transfer of personal data, including whistle-blowing reports to the U.S.).

Therefore, if the transfer agreement contains the EU Standard Contractual Clauses, or if the multi-national group of companies has adopted internal rules that have previously acknowledged that they guarantee an adequate level of protection of privacy and fundamental rights of individuals, the transfer of whistle-blowing reports containing personal data is authorized outside the EEA.

In addition, it is only if the whistle-blowing policy and its scope meet the requirements of this Deliberation of the CNIL that would automatically allow the transfer of whistle-blowing reports containing personal data.

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- Data Protection Act 1978 (English version)
- French Labour Code (e.g., Article L.2323-32; Article L.1121-1)
- French case law
- CNIL ("the CNIL in a nutshell")

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

Yes. If evidence is gathered illegally, it cannot be presented in court in dismissal cases or in support of a dismissal.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

The Works Council must be informed and consulted prior to any decision regarding the implementation within a company of a system to monitor employees. This is not co-determination, as the Works Council's opinion is not binding. The challenge is to get the opinion; once the Works Council delivers it, whether it is negative or positive, the monitoring can take place.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

The principle of express consent may constitute a major change, which is different from the current rules surrounding preliminary information of the employee.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

An employer may face criminal penalties including both fines and imprisonment. These vary depending on the offence, although large fines may be imposed for unauthorised recording; invasion of privacy; violation of secrecy of correspondence; failure to notify the CNIL of a personal data processing system; and the fraudulent collection, unfair, or illegal use of personal data.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

For abusive language or insulting remarks made via social media or on Facebook against an employer, colleague, or manager, the French case law draws a distinction between the public and private sphere. If an employee's Facebook page is public, the abusive language can constitute reason for termination of employment in certain circumstances. In such cases, it has been held by local courts that the employee exceeded his/her freedom of expression. On the other hand, if the Facebook page is private and access is limited to friends and family, the Courts may consider any comments made to be part of the employee's right to free speech.

It is important to note that the French Supreme Court has not yet ruled on this issue; thus, the law has not yet developed to a stage where it can be said that the photographs or comments would allow for termination for cause or give the employee an entitlement to severance. Generally, the termination must be for disciplinary reasons, but the entitlement to severance will depend on the seriousness of the misconduct or expressions.

The Court of Appeal has held that, if an employee makes an insulting comment regarding his/her employer or a colleague on his/her Facebook page, but does not refer to either by name, it is not a gross misconduct, but only a termination for cause.

For more information about transferring personal data in France, please contact:

Sophie Pélicier Loevenbruck
Fromont Briens
T: +33 (0)1 44 51 63 80
sophie.pelicier@fromont-briens.com
www.fromont-briens.com

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

Provided there is a statutory basis, the collection and transfer of personal data in Germany to a country outside the EEA shall be lawful. The Federal Data Protection Act (FDPA) provides that an adequate level of prior consent of the data subject is necessary if the transfer cannot be justified by statute.

For a transfer of data to a third country outside the EEA, the recipient must ensure a sufficient level of data protection. This requirement shall be met if: an employee gives his/her consent to the transfer (this is not practical in most cases, since the consent can be withdrawn at any time); the EU Commission has officially recognised that the recipient country has adequate protection; the transfer is under the EU Standard Contractual Clauses; or the transfer is under Binding Corporate Rules. Safe Harbour Certification may no longer be used because the European Court of Justice ruled the Safe Harbour Programe "invalid" on October 6, 2015. Consultation and approval by a data privacy agency may be required.

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

In general, an employer would not require national authorisation if the data is being transferred through use of the EU Standard Contractual Clauses. However, it is important to note that the FDPA is also applicable.

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

There are no specific rules that concern the transfer of whistle-blowing reports or whistle-blower data within multinational corporations. Under the FDPA, personal data may be collected and processed where necessary for employment-related purposes under a contract of employment, or used to detect crimes where there is reason to believe the data subject has committed an illegal act in the course of his/her employment. The reasons for using such data must be balanced and proportionate against the data subject's legitimate interests.

The collection and transfer of personal data to fulfil a company's own business purposes shall also be allowed under the FDPA insofar as it is necessary to safeguard justified interests of the controller, and there is no reason to assume that the data subject has an overriding legitimate interest in his/her data being excluded.

The prior consent of the employee/whistle-blower charged with misconduct can serve as the legal basis for the transfer. However, this may not be a practical solution in situations where the misconduct of employees is being investigated. Further, consent can be withdrawn at any time. As such, a works agreement on a corporate whistle-blowing system can also provide a legal basis for transferring personal data. It is important to note that establishing a corporate code of conduct, which often includes a whistle-blower hotline, is subject to co-determination of the Works Council.

CONTENTS

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- The Constitution of the Federal Republic of Germany
- Federal Data Protection Act
- Works Constitution Act
- Civil Code

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

The German legal system does not have a comparable principle. However, the courts do place an emphasis on the fact that using illegally gathered evidence in the courtroom could be an unlawful violation of personal rights. In cases where such evidence may play a role, the court will balance the need to use the evidence against the interest of the data subject to protect his/her privacy. However, there has been a tendency of the Courts not to use evidence that has been gathered in such a way.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

Works Councils can claim comprehensive information, consultation, and even a co-determination right in connection with monitoring employees under the Works Constitution Act. The most important right of co-determination is triggered if a company introduces a technical system designed to monitor the behaviour or performance of the employees at work. This includes video surveillance, GPS, or time-tracking systems. Co-determination means that the company needs to have the Works Council agree with the monitoring or allow for a Conciliation Committee – a form of internal arbitration body – to decide on the monitoring.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

There probably will be no substantial changes that will impact the legal framework of monitoring employees. However, it is likely that the consent-principle will probably not survive under the new regulation.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

The law on data protection provides that illegal monitoring of employees can be an administrative offence and/or a criminal act. German data protection agencies can be aggressive in their investigations and penalties for data protection violations, issuing fines up to € 1.3 million. It is important to also note that, if an employer violates an employee's privacy rights, the employee may be able to sue for damages.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

With regard to posting incriminating photographs, there has been no comparable case within the German labour courts; therefore, no precedent exists. However, termination with notice, which is based on the employee's behaviour, may be enforceable. If a photograph shows an employee seriously breaching his/her contractual duties, which then results in reputable damage to the company in a public forum, the employer could argue that, if termination is not allowed, similar incidents might occur in the future. A prior warning, which is generally required before termination, would not be required in this instance due to the seriousness of the misconduct. However, the employee must know that the employer would not accept this kind of behaviour. Therefore, it is advisable for the employer to have in place a clear social media policy.

A termination without notice may also be enforceable for employees who post on Facebook or other social media derogatory or disparaging remarks about other employees. There is no indication that the employer must consider other less serious options to discipline the employee. In particular, a prior warning is not required, as the employee should have known his/her behaviour was unacceptable.

The labour courts have accepted defamation of the employer or colleagues on social media as a reason to terminate with notice. It does not make a difference if the employee has specifically named anyone or not; the labour courts have taken the view that if family, friends, and/or third parties can make a connection to the company when reading the insult, this can directly link the comments to the employment relationship. Termination without notice may be enforceable, but would have to be decided on a case-by-case basis depending on the severity of the comments, e.g., if related to race or gender discrimination.

For more information about transferring personal data in Germany, please contact:

Jan Tibor Lelley
Buse Heberer Fromm
T: +49 (0) 69 989 7235 0
lelley@buse.de
www.buse.de

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

The transfer of personal data is permitted to a non-member state of the European Union following a permit granted by the Data Protection Authority (DPA) if it deems that the country in question guarantees an adequate level of protection. For this purpose, it shall take into account the nature of the data, the purpose and duration of the processing, the relevant general and particular rules of law, the codes of conduct, and the security measures for the protection of personal data, as well as the protection level in the countries of origin, transit, and final destination of the data.

A permit is not required when the Standard Contractual Clauses are approved by the European Commission (Model Clauses), as well as when the Binding Corporate Rules have been executed.

The transfer of personal data to a non-member state of the European Union that does not ensure an adequate level of protection is exceptionally allowed following authorization from the DPA, provided that one or more of the following conditions occur:

- The data subject has consented to such transfer, unless such consent has been extracted in a manner contrary to the law or bonos mores;
- The transfer is necessary to protect the vital interests of the data subject, provided he/she is physically or legally incapable of giving consent for the conclusion and performance of a contract between the data subject and the data controller, or between the data controller and a third party in the interest of the data subject, or for the implementation of pre-contractual measures taken in response to the data subject's request;
- The transfer is necessary to address an exceptional need and safeguard a superior public interest, especially for the performance of a co-operation agreement with the public authorities of the other country, provided that the data controller provides adequate safeguards with respect to the protection of privacy and fundamental liberties, and the exercise of the corresponding rights transfer is necessary for the establishment, exercise, or defence of a right in court;
- The transfer is made from a public register, which by law is intended to provide information to the public and is accessible by the public or any person who can demonstrate a legitimate interest, provided the conditions set out by law for access to such a register are in each particular case fulfilled;
- The data controller shall provide adequate safeguards with respect to protecting the data subjects' personal data and the exercise of their rights when the safeguards arise from conventional clauses that are in accordance with the regulations of the Law.

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

No authorization is needed; only notification to the DPA is required.

CONTENTS

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

According to Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data, implementing Directive 95/46/EC, the local Data Protection Authority should always be notified about the establishment of a file or, in general, personal data processing through the operation of a hotline. Although the anonymity on the reporting employee is usually preserved, the reported employee is not anonymous.

Further, when collecting and processing sensitive personal data or transferring (sensitive/non-sensitive) personal data outside the EU, the Greek subsidiary should also request relevant authorization from the DPA.

However, especially in cases where an EU Standard Model Clauses Agreement has been concluded between the data importer and the Greek entity, a simple notification is sufficient; there is no need to request authorization from the DPA.

Following the decision of October 6, 2015 (C-362/14), the European Court of Justice ruled that the level of data privacy protection according to the U.S. Safe Harbor Certification is inadequate and that the Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the U.S. Department of Commerce is invalid.

Therefore, any personal data transfer from companies in the EU/EEA to the U.S. under the previous regime of Safe Harbor, is currently in lack of a legal basis. For the time being, according to the Directive 95/46/EC, such transfer may continue to be carried out by using the remaining tools that still ensure an adequate level of protection, i.e., by the execution of Binding Corporate Rules or the conclusion of EU Standard Model Clauses Agreements.

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- Greek Constitution (articles 9, 19)
- Data Protection Law 2472/1997, as validly in force today
- Law 3471/2006 "On the protection of personal data and privacy in the field of electronic communications"
- Directive 115/2001 of the Data Protection Authority
- Criminal Code
- Civil Code

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

The Greek Constitution explicitly forbids, before any court (civil, criminal, administrative) and in any procedure, the use, by any means, of evidence obtained through illegal processing of personal data or by violating the privacy of correspondence. The legislator considered that the protection of personal data, as well as the protection of the confidentiality of correspondence would be worthless if not accompanied by a corresponding procedural dimension. Although it is up to the Labour Court to freely evaluate and admit unlawfully obtained evidence in the context of a dismissal case, this does not cure the criminal implications and does not release the person who has illegally obtained such evidence from the offences committed.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

According to DPA Decision 115/2001, employee representatives should be informed and have the opportunity to express their opinion prior to the introduction of control and monitoring methods.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

We do not expect it will. The Greek DPA has repeatedly ruled that monitoring of the working place insults employees' rights to privacy and is contrary to the principle of proportionality, as defined in the Greek Constitution.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

The data protection legislation provides for administrative and penal sanctions that vary according to the gravity of the breach. Administrative sanctions (such as warning, fines, temporary/permanent revocation of permit, destruction of the file, or ban of processing) are imposed by the Data Protection Authority following a hearing of the Data Controller or its representative, whereas penal sanctions (imprisonment and/or monetary fines) can be imposed.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

The facts have to be evaluated so that the employer can prove that an employee's negative comments constitute misconduct/non-contractual behaviour or that they have otherwise caused damage to the employer. Dismissal has to be justified. The gravity of the comments is decisive in judging whether the element of loyalty/trust, which should exist in the employment relationship between the employer and employee, has ceased to exist.

Employees are expected to be careful when expressing themselves on social media, due to their general duty of loyalty towards their employer during the term of their employment relationship. Freedom of speech may have to be restricted up to the limit where it could conflict with the duty of loyalty and the interests of the employer. A potential liability arises for the employer stemming from an employee's behaviour online, even where the employee posts them during his/her personal time or from home, since the employee's comments could be discriminatory, defamatory, insulting etc. Where the employer can prove that such comments damaged its image and/or reputation, and are publicly available, such activity by an employee could constitute a valid reason for termination.

For more information about transferring personal data in Greece, please contact:

Effie Mitsopoulou
KYRIAKIDES GEORGOPOULOS LAW FIRM
T: +30 210 817 1500
e.mitsopoulou@kglawfirm.gr
kg.law@kglawfirm.gr
www.kglawfirm.gr

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

The transfer of personal data outside the EEA is lawful to countries that can ensure an adequate level of protection. Until recently, U.S. entities certified under the EU-U.S. Safe Harbour regime were considered to ensure an adequate level of protection, but a recent decision of the Court of Justice of the European Union (In Case C 362/14, Maximillian Schrems v Data Protection Commissioner) (the CJEU Decision) ruled that this is not the case. Therefore, transfers to the U.S. must be legitimised on other grounds if they are to be lawful.

Some notable exceptions to the prohibition on transfer outside of the EEA include: where the transfer is necessary for the conclusion or performance of a contract to which the data subject is a party; or between the data controller and someone other than the data subject, but at the data subject's request; the transfer has been authorised by the Irish Data Protection Commissioner (the DPC); the transfer takes place by virtue of the EU Standard Contractual Clauses or Corporate Binding Rules; the data subject has consented to the transfer; the transfer is required or authorised by law; or the transfer is to a country that has been pre-approved by the European Commission. The DPA also sets forth additional exceptions under which the transfer of data may be permitted.

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

The transfer of personal data to a country that does not provide an adequate level of protection is permitted when the EU Standard Contractual Clauses (commonly referred to in Ireland as the "model contracts") are used to facilitate the transfer. No additional authorisation is required unless the provisions of the Clauses are varied. The DPC has the power to endorse variations to the EU Standard Contractual Clauses specific to Irish circumstances.

As of December 2015, the DPC has not issued any guidance as to whether it considers the efficacy of EU Standard Contractual Clauses to be undermined by the CJEU Decision. Model contracts remain valid and thus they can continue to be used for as long as the Commission decision approving them remains in force. However, the CJEU Decision has made it clear that national data protection authorities are obliged to review the adequacy of protection afforded by third countries, even where there is a Commission decision as to adequacy in place, such as the decision in relation to the EU Standard Contractual Clauses (Commission Decision C(2001) 497 (amended by Commission Decision C(2004) 5271) and Commission Decision C(2010) 593).

Some data protection authorities have started to call the validity of the EU Standard Contractual Clauses into question and expressed the view that they cannot be used as an alternative to Safe Harbour without additional safeguards; however, only the CJEU can declare the Clauses invalid. The Article 29 Working Party

CONTENTS

(an independent advisory group set up under the EU Data Protection Directive) has recently (on 16 October 2015) issued guidance, which confirms that, pending further analysis by the Working Party on the impact of the CJEU Decision, the EU data protection authorities consider that the EU Standard Contractual Clauses and Corporate Binding Rules can still be used. This will not, however, prevent data protection authorities from investigating particular transfers and exercising their powers to investigate individual complaints.

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

In addition to satisfying one of the conditions for legitimising the transfer referred to above, organisations must also ensure that their whistle-blowing scheme complies with the other requirements of the DPA in relation to the processing of personal data. Any personal data must be obtained and processed fairly and lawfully for one or more specified, explicit, and legitimate purposes; used and disclosed only in ways compatible with that purpose; be accurate, complete, and up-to-date and adequate, relevant, and not excessive in relation to the purpose for which it was collected; be kept secure; and not kept for any longer than is necessary for those purposes. The scheme must also satisfy the grounds for legitimising processing as set out in Section 2A of the DPA.

Complying with the foreign legal obligations, such as the Sarbanes-Oxley Act, will not justify the establishment of a whistle-blowing scheme. The relevant legal obligation must be one imposed by Irish law or the Community. However, it may be justified if it can be shown that the transfer is for a legitimate interest of an employer, provided that a balance is struck between the controller's legitimate interest and the fundamental rights of the data subject.

The DPC has recommended adherence to Article 29 Working Group Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, and banking and financial crime.

In Ireland, whistle-blowers are protected by the Protected Disclosures Act 2014. This Act protects the identity of the whistle-blower (subject to some limited exceptions) and any transfer of information must respect that requirement.

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- The DPA
- The Irish Constitution

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

In circumstances where evidence has been gathered by covert surveillance, it has been held by the Irish Employment Appeals Tribunal that the dismissal was unfair, as the use of such evidence was not in accordance with fair procedures.

Employers should be transparent with all monitoring. As such, they should inform employees that monitoring is taking place, and further state in their disciplinary policies that evidence obtained by way of monitoring may be used in a disciplinary process to ensure compliance with the principle of fair procedures. Only in exceptional circumstances associated with a criminal investigation should they use covert surveillance.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

In general, no rights exist. An employer is free to introduce monitoring into the workplace in pursuit of a legitimate interest. However, these interests cannot take precedence over the principles of data protection.

If an employer has chosen to recognise a trade union for collective bargaining, then, subject to the rules of the collective bargaining agreement in place between the organisation and the trade union, the employer may be committed to consulting the union before introducing any such measure.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

The terms of the draft General Data Protection Regulations (the Draft Regulation) are currently (December 2015) being negotiated between the three main institutions of the EU (Parliament, Council, and the Commission) but the approaches put forward so far would indicate that there will be changes to the legal landscape in respect of monitoring employees. A recent approach adopted by the Council on 15 June 2015 and recommendations from the European Data Protection Supervisor (EDPS) issued on 27 July 2015 provide for changes to the requirement for consent to legitimise the processing of personal data. Currently under the Irish DPA, consent can be obtained to legitimise the processing of personal data, but the DPA does not specify the level of consent required. This may vary from case to case and between implied and explicit consent. Where consent will be relied upon, the Council suggests unambiguous consent should be obtained by clear affirmative action on the part of the data subject, whereas the EDPS recommends that consent should be explicitly provided.

The Council and the EDPS have also suggested that the Draft Regulation should provide that Member States may, by law, provide for specific rules around the processing of employee personal data in the employment context. However, the EDPS is more restrictive in this suggestion, recommending that it be implemented only within the limits of the Draft Regulation.

Additionally, the Draft Regulation could bring into force increased fines for breach of data protection legislation, including proposals for financial penalties to be set by reference to a de minimum amount or a percentage of annual worldwide turnover of the company.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

Civil sanctions: Under the DPA, a data controller or a data processor, shall, so far as regards the collection by him of personal data or information intended for inclusion in such data or his dealing with such data, owe a duty of care to the data subject concerned. An individual may apply to the courts in order to bring a civil action against the data controller or data processor for failure of its duty of care. A breach of such duty by a data controller or data processor can result in an award of damages, but the DPA does not provide for an automatic award of damages for a breach of the DPAs, and proof of damage is necessary where such a claim is made.

In addition, the DPC must investigate any complaints that he receives from individuals who feel that personal information about them is not being treated in accordance with the DPA, unless he is of the opinion that such complaints are frivolous or vexatious. The DPC has the power to conduct onsite inspections, issue an information or enforcement notice (requiring the provision of information or data to be blocked, rectified, erased, or destroyed) and prohibit the transfer of personal data outside the EEA.

Individuals may be entitled to take an action for breach of their constitutional rights to privacy under the Constitution.

Criminal sanctions: A person guilty of an offence under the DPA shall be liable on summary conviction to a fine not exceeding € 3,000 or, on conviction or indictment, to a fine not exceeding € 100,000. Directors, managers, secretaries, and other officers of an entity may be guilty of an offence where the entity commits an offence with the consent or connivance of the relevant person or it is attributable to his/her neglect.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

Dismissal for gross misconduct is an available option in response to an employee posting inappropriate and disparaging photographs of or comments about other employees, particularly where the subject is identified and where damage to the employer's reputation has occurred. Where the employee is not identifiable, the employer may not be in a position to conclude who committed the gross misconduct.

Dismissal for misconduct is permissible under Irish law. However where an employee has 12 months' service, all dismissals are presumed unfair, unless an employer can demonstrate that it followed a fair disciplinary process and the decision to dismiss was proportionate. Essentially, the Irish Employment Appeals Tribunal expects employers to consider all alternatives to a dismissal prior to issuing the sanction to dismiss.

An employer may struggle to demonstrate that dismissal was a proportionate response to insulting or derogatory Facebook postings or comments, unless it can prove: the comments had a damaging effect on its reputation; the company had a social media policy in place with adequate training outlining what is and is not appropriate use of personal social media sites; or, under the circumstances, it is reasonable to dismiss the employee. The Irish Employment Appeals Tribunal has accepted that the sanction of dismissal is fair in circumstances where an employee's posts are offensive, resulting in a breakdown of trust of such significance that the employee's employment becomes untenable.

For more information about transferring personal data in Ireland, please contact:

Duncan Inverarity
A&L Goodbody
T: +353 1 649 2401
dinverarity@algoodbody.com
www.algoodbody.com

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

According to the Italian Personal Data Protection Code, the transfer of personal data to a third-party country outside the European Union can take place if the transfer falls within the scope of a "permitted transfer" under the Code (e.g., the data subject has given his/her consent; the transfer is necessary for the performance of an obligation resulting from a contract to which the data subject is a party, etc.) or if the transfer is authorised by the Italian Data Protection Authority (the Garante) on the basis of adequate safeguards for data subjects' rights. Unless the transfer falls into one of these categories, it shall be prohibited if the third country does not ensure an adequate level of protection.

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

Transfer of personal data to a country that does not provide an adequate level of protection is allowed when the Standard Contractual Clauses issued by the European Commission are incorporated into an agreement. There is no need to obtain any national authorisation, provided there are no amendments.

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

Under Italian Law the transfer of whistle-blowing reports containing personal data to a third-party country outside of the European Union can take place only in the situations mentioned above.

In the light of such provisions, it is necessary to ascertain the purpose for the transfer of the whistle-blowing reports to verify whether or not it is a "permitted transfer." Also, on a case-by- case basis, local subsidiaries are allowed to transfer whistle-blowing reports containing personal data only if they obtain the consent of the employees in writing, due to the possible presence of sensitive data, or if the subsidiary has requested a specific authorization to the Garante or used EU Standard Contractual Clauses.

CONTENTS

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

Pursuant to Italian Law, the monitoring of employees is regulated by the Statute of Workers (section 4). This provision has been amended by the Legislative Decree no. 151/2015 entered into force on September 24, 2015. According to the new provisions, the instruments and equipment that are potentially able to also monitor employees are permitted only to the extent they are required for organizational, productive, or safety reasons or for safeguarding company assets, and provided that their use is agreed to by the Work Council/ most representative Trade Unions or authorized by the Labor Office, depending on the specific case. The new provisions specify that such rules do not apply (thus, no agreement or authorization is needed) to the instruments/equipment that are used by the employees for performing their activity (e.g., laptop, mobile phone) and to devices that are used by the employer to register the employees' accesses and attendance at the workplace. In addition, the data and the information collected through such instruments/equipment can be used for all purposes related to the employment relationship provided that the employees have been adequately informed about how the instruments must be used and how the controls can be carried out, in compliance with Data Protection legislation.

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

Italian law does have a similar principle. If evidence of misconduct or breach of contractual duties is gathered by unlawfully monitoring employees, the evidence cannot be used in a subsequent trial to prove an employee's misconduct. Furthermore, according to case law, monitoring employees is deemed to be lawful to the extent it is carried out to protect the company's property and reputation.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

As stated above, as provided by Section 4 of the Workers' Statute, an agreement with the Work Councils/ Trade Unions or the authorization from the Labor Office is needed to install monitoring systems for organizational, productive, or safety reasons or for safeguarding company assets, including if the monitoring systems are used to also monitor the working activity by remote control (which is not allowed). If the monitoring systems (e.g., cameras) are installed to control an area/room to which employees do not have access, it is not necessary to get agreement from the Work Councils/Trade Unions or the authorization of the Labor Office.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

It is likely that the upcoming EU data privacy/data protection regulation will be limited to mere "data privacy" issues and that it won't modify the current legislation on the possibility to monitor employees. Therefore, it should not have a high impact on the legal landscape in Italy.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

In case of a breach of provisions set forth by the Statute of Workers, the employer may be subject to a fine or face imprisonment of up to one year. In some cases, the judge can also order the publication of the judgment in the newspapers.

The employee may also claim for damages if he/she has suffered any damages as a consequence of the processing of personal data.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

If the incriminating photographs are taken at the workplace, this may be a reason for termination, although this would also depend on how the employer obtained the pictures. Posting inappropriate or insulting Facebook comments may also be ground for termination, as the employee has expressed negative comments regarding the company. However, such an evaluation should be made on a case-by-case basis, taking into account the privacy settings on the employee's Facebook profile and whether the name of the company can be identified based on the information the employee has put on Facebook.

In the absence of any legislation regarding the use of social media by employees, and considering its increasing prevalence, some multinational companies have implemented policies addressing its use, which can help when taking disciplinary action against an employee.

Under Italian Law, an employee can be dismissed for just cause if the cause is so serious as to not allow for the continuation of the employment relationship. This would mean that the employee is terminated without notice. Furthermore, although an employee may be dismissed also for a justified subjective reason, whereby he/she commits a serious violation of his/her contractual obligations, but not so serious as to represent a just cause for dismissal (i.e., termination with notice), the cases where employees post incriminating photographs or derogatory or insulting comments are more likely to fall under the dismissal for just cause mentioned above.

For more information about transferring personal data in Italy, please contact:

Angelo Zambelli
Grimaldi Studio Legale
T: +39 02 3030 9390
azambelli@grimaldilex.com
www.grimaldilex.com

Silva Annovazzi
Grimaldi Studio Legale
T: +39 02 3030 9303
sannovazzi@grimaldilex.com
www.grimaldilex.com

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

Under the Luxembourg data protection law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data as amended (the Data Protection Law), a distinction is made between the authorised transfer of personal data to countries that ensure an adequate level of protection and those that do not. The latter is in principle prohibited unless one of the exceptions listed in the Data Protection Law applies. The United States is considered not to provide an adequate level of protection. The fact that the U.S. recipient complies with the Safe Harbour Principles would not prevent it from being subject to claims that such data transfers are unlawful. Indeed, the Court of Justice of the European Union declared the EU-U.S. Safe Harbor framework invalid as a mechanism to legitimize transfers of personal data from the EU to the U.S. (Case C-362/14 Maximillian Schrems v Data Protection Commissioner, 6 October 2015).

There are several commonly used exceptions for the transfer of employee personal data to a country that does not offer an adequate level of protection equivalent to that offered in the EEA, including the prior authorisation of the Luxembourg Data Protection Authority (the CNPD), based on EU Standard Contractual Clauses or Binding Corporate Rules.

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

Under the Data Protection Law, the use of EU Standard Contractual Clauses is subject to the prior authorisation of the CNPD. A copy of the agreement incorporating the EU Standard Contractual Clauses, together with the completed corresponding authorisation request form (available on the CNPD website), must be provided when filing the authorisation request.

If the Standard Contractual Clauses are amended, the CNPD must analyse such amendments to ensure that adequate safeguards with respect to protecting the privacy and fundamental rights and freedoms of the employees and the exercise of their rights are foreseen.

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

As mentioned above, the employer must first obtain authorisation from the CNPD prior to the data transfers (whether based on EU Standard Contractual Clauses or Binding Corporate Rules). The data transfers must also comply with the general principles of adequacy and proportionality, which must be assessed on a case-by-case basis.

The CNPD has not issued any guidelines for the transfer of data collected in the context of whistle-blowing.

CONTENTS

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- The Data Protection Law (French/English)
- The Labour Code
- The Luxembourg Law of 30 May 2005 relating to the Protection of Persons with regard to the Processing of Personal Data in the electronic communication sector, as amended (French/English)

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

In principle, evidence obtained illegally cannot be presented in court. However, the Luxembourg courts have acknowledged the possibility for a judge to assess, in limited circumstances, the admissibility of evidence gathered illegally.

As such, the Luxembourg Court of Cassation deemed that, in assessing such admissibility, the judge must take into consideration all the elements of the case in its entirety, including the method by which the evidence was gathered and the circumstances under which the unlawfulness was carried out.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

In principle, employee representatives have a right to information regarding the monitoring of employees under the Labour Code. A co-determination right of the joint committee, if any, may also exist, depending on the legitimacy basis of the monitoring.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

At this time, it is difficult to assess the impact of the upcoming data protection regulation on the Luxembourg legal landscape regarding the monitoring of employees because no public guidelines have yet been issued.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

Non-compliance with the provisions of the Data Protection Law and the Labour Code on monitoring is subject to criminal sanctions, including fines of up to € 125.000 and/or imprisonment of up to one year. A court could also order a permanent ban on the monitoring if it is in breach of the legal provisions.

The data subject may also enforce his/her rights under the Data Protection Law by filing a cessation action or a civil claim for damages on the basis of the Civil Code provisions. However, there is currently no published case law to the best of our knowledge that grants damages to an employee following non-compliance with the legal provisions on monitoring.

Finally, the CNPD may also impose administrative sanctions, although this does not include administrative fines.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

Posting incriminating photographs of other employees on Facebook or elsewhere without their consent most likely would be considered good reason to terminate the employment agreement with immediate effect, depending on the detailed circumstances, since continuing the employment relationship is likely to be immediately and definitely impossible.

An issue may arise for any derogatory or disparaging comments made on Facebook with regard to evidence if an employee does not specifically name the company or the subject of the photo. Although the statement is likely to be considered a good reason to terminate the employment agreement with immediate effect for important reason, the challenge will be to prove the link to the employer. A termination with notice might be more appropriate to mitigate the employer's risk of unlawful termination.

For more information about transferring personal data in Luxembourg, please contact:

Louis Berns
Arendt & Medernach SA
T: +352 40 78 78 240
louis.berns@arendt.com
www.arendt.com

Héloïse Bock
Arendt & Medernach SA
T: +352 40 78 78 321
heloise.bock@arendt.com
www.arendt.com

Philippe Schmit
Arendt & Medernach SA
T: +352 40 78 78 393
philippe.schmit@arendt.com
www.arendt.com

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

Under Maltese Law, the transfer of data to a third country may occur subject to the provisions of the Data Protection Act and provided the country receiving the data enjoys an adequate level of protection. The Act further states that the adequacy of protection of a third country shall be evaluated vis-à-vis all the circumstances concerning a data transfer operation.

In particular, the Legislation in force in Malta provides that the Data Controller (i.e., the person who alone or jointly with others determines the purposes and means of processing personal data) must notify the Commissioner of any transfer of data resulting from a processing operation. Any person who contravenes or fails to comply with these regulations is liable for administrative fines.

In light of the CJEU's recent ruling in the case of Maximillian Schrems v Data Protection Commissioner, the Maltese Office of the Information and Data Protection Commissioner has held that this ruling necessitates that the national competent authorities, including the Maltese Data Protection Commissioner, will now have to intensively review requests that are made by data subjects with respect to the transfer and handling of their data by U.S. companies. Furthermore, data controllers who have been previously transferring data to the U.S. in line with the Safe Harbour Rules are now obliged to utilise other suitable mechanisms to safeguard the transfer.

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

The use of Standard Contractual Clauses is highly commended to guarantee that the rights of individuals are protected. The Information and Data Protection Commissioner (Commissioner) has the right to decide whether a third country provides an adequate level of protection and, if not, can prohibit the transfer.

Generally, EU Member States are obliged to acknowledge the use of EU Standard Contractual Clauses that are accepted by the Commissioner. As such, Member States may not decline a transfer of data. However, in Malta, because the Commissioner has the authority to ultimately decide whether a third country offers adequate protection regarding data transfers, if he/she decides that a particular country does not in fact provide satisfactory protection, the transfer is barred.

CONTENTS

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

Locally, the Data Protection Act provides that a transfer of personal data that is subject to processing or intended processing may be transferred to a third country according to the provisions of the Act. The transfer must comply with the criteria set out in the Act and may be subject to processing only upon fulfilment of the following criteria:

- When the Minister in charge of data orders the transfer to be made anyway;
- The data subject has given unambiguous consent;
- Where the processing is necessary for the data subject and controller for pre-contractual or contractual purposes;
- Where the public interest is involved, such as where somebody makes a legal claim;
- To protect the vital interests of the data subject; where the information is available to others by law under certain conditions; and
- Where the Commissioner establishes conditions with the third country to ensure a better level of protection.

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- Data Protection Act (CAP 440)
- Processing of Personal Data for Electronic Communications Sector (SL 440.01)
- Notification and Fees (Data Protection Act) Regulations (SL 440.02)
- Third Country (Data Protection Act) Regulations (SL 440.03)
- Processing of Personal Data (Protection of Minors) Regulations (SL 440.04)
- Data Protection (Processing of Personal Data in the Police Sector) Regulations (SL 440.05)
- Processing of Personal Data (Police and Judicial Cooperation in Criminal Matters) Regulations (SL 440.06)
- Transfer of Personal Data to Third Countries Order (SL 440.07)

Directive 95/46/EC on data protection (Data Protection Directive) has been transposed into Maltese law through various the regulations above and in particular through the Data Protection Act (EU Legislation on Data Protection).

The right to privacy is also enshrined in the Constitution of Malta.

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

The gathering of illegal evidence is not dealt with directly by local laws. However, the concept of "best evidence" is often used.

The Information and Data Protection Tribunal may summon any person to appear before it, and produce evidence and forward the necessary documents. Furthermore, the rules of evidence within the workings of a tribunal are not specifically laid out; in fact, the Tribunal is allowed to regulate itself procedurally.

If a party to a case is not satisfied with the decision, it can appeal within 30 days. The Court of Appeal is regulated under the code of Organisation and Civil Procedure, which provides that evidence that is considered irrelevant or superfluous may be disallowed or thrown out where it is deemed not to be the best evidence the party may produce. The admissibility of evidence rules are invoked to safeguard the Maltese judicial system and to ensure that the best evidence is produced along with true evidence.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

The Data Protection Act provides for a "personal data representative," who has the power to ensure that data is processed lawfully and correctly. The representative is appointed by the controller of personal data and exercises his role independently. The representative must ensure that data is processed in line with the rules of good practice and if he/she is not satisfied with a particular data process he/she is obliged to point out the shortcomings to the controller of personal data. In any case of doubt regarding compliance, the representative can raise the issue with the Commissioner. The same shall apply if the proper application of the processing of personal data is not clear.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

Currently the concept of "Blanket Consent" is applied with regard to monitoring employees. However, with the coming into force of the new data protection regulation, "Blanket Consent" shall be replaced by "Purpose Consent."

Blanket Consent refers to consent that does not pertain to a particular data process, but instead to consent that is given across the board.

On the other hand, Purpose Consent is obtained for a specific data process. At present, upon the commencement of employment an entity acquires the data subject's consent, which does not have to be detailed or restricted by time. With the advent of this new requisite type of consent, a data subject who has provided his/her consent to data processing is not deemed to be absolute. In fact, the prior consent given by the data subject is no longer valid upon the fulfilment of a particular data process or task.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

Illegal monitoring of employees is not specifically listed in the relevant sections of the Data Protection Act that address court penalties and administrative fines. However, the Act does provide for those offences that are not specified in the latter Schedules. Thus, a person who is guilty of an offence relating to any provision within the Data Protection Act shall be liable to a fine of not less than € 120 and not more than € 23,300, to imprisonment for six months, or both.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

Employers may be damaged by inappropriate use of social media by their employees, for example, when:

- An employer is the victim of an employee's criminal offence;
- An employee's use of social networking sites damages the employer's business reputation or the employee releases confidential information;
- An employee's bullying is carried out on the internet and/or mobile phones through social networking sites, email, and texts.

In such cases, the employer may dismiss the employee.

In particular, Maltese case law indicates that the Tribunal favours cases for dismissal where the employer has given the necessary warnings to an employee. Three written warnings are generally considered customary. If the employee continues to persist with his/her unacceptable behaviour, the employer may dismiss him/her on the basis of good and sufficient cause. Before being dismissed, the employee is usually requested to provide the employer with his/her justification with respect to the alleged facts.

The Tribunal has continuously held that negative or offensive comments conveyed on social media platforms in relation to an employer may be deemed a fair dismissal since the employee's offensive behaviour might hinder the reputation of the employer and his/her business. Moreover, misconduct conveyed on social media may also occur in the form of insulting comments towards an employer's customers, which may consequently damage the employer's reputation and business relations with third parties.

If an employer lawfully dismisses an employee on good and sufficient cause, the employer is not obliged to compensate the employee for any wages concerning such notice period. Local legislation does not define the term "good and sufficient causes." In fact, the Law only provides a list of reasons that are not acceptable grounds for dismissal, for example, the employee was a member of a trade union, is pregnant, etc.

For more information about transferring personal data in Malta, please contact:

Andrew J. Zammit
CSB Advocates
T: +356 2557 2300
ajz@csb-advocates.com
www.csb-advocates.com

Ann M. Bugeja
CSB Advocates
T: +356 2557 2300
amb@csb-advocates.com
www.csb-advocates.com

Angela Bruno
CSB Advocates
T: +356 2557 2300
abr@csb-advocates.com
www.csb-advocates.com

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

As in other EU and EEA member states, personal data may only be transferred from a Norwegian subsidiary to countries outside the EEA that ensure an "adequate level of protection" pursuant to article 25 of the data protection directive (95/46/EU). By way of derogation, such transfers may nonetheless take place if the data subject has given his or her consent, the transfer is necessary for performance of a contract, etc. Also, the Norwegian Data Protection Authority may authorize the transfer on the basis of the EU model clause. Alternately the companies may adopt Binding Corporate Rules.

Until recently, Norwegian data protection authorities also considered Safe Harbor-certification of U.S. companies to provide an "adequate level of protection." This is, however, no longer the case. In C 362/14 (Maximillian Schrems v Data Protection Commissioner case), the European Court of Justice held that the Safe-Harbour agreements are no longer deemed to be in accordance with EU data protection laws. The court also held that national regulatory authorities may examine with complete independence whether the transfer of a person's data to a third country complies with the Data Protection Directive.

The ruling does not provide direct guidance on the consequences for Safe Harbor-certified companies. The Norwegian Data Protection Authority is a member of the Article 29 Working Party, which has urgently called on the Member States and the European institutions to open discussions with U.S. authorities in order to find political, legal, and technical solutions enabling data transfers to the U.S. Further, it will also analyse the impact on other transfer tools, such as the Standard Contractual Clauses and Binding Corporate Rules.

Until a new agreement or mechanism is negotiated, the Norwegian Data Protection Authority has publicly stated that Norwegian companies may not transfer personal data to the U.S. on the basis of the Safe Harbor arrangement. Until the Working Party finalizes its analyses, the Standard Contractual Clause and the Binding Corporate Rules can still be used. The Authority may also consent to the transfer of personal data on an individual basis.

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

The data controller (i.e., Umpire) should notify the NDPA before processing personal data by automatic means or establishing a manual personal data filing system that contains sensitive personal data. Notification should be given no later than 30 days prior to commencement of the processing. The NDPA will give the controller a receipt of notification.

Whistle-blowing reports may contain information regarded as sensitive. According to Norwegian law, the transfer of such information is subject to concession from the NDPA, thus requiring a more accurate evaluation of the content of the whistle-blowing reports.

CONTENTS

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

If the given report merely contains personal data, the transfer will be legal if the receiver of the information provides sufficient guarantees for protecting the data and the NDPA is notified. With regard to sensitive personal data, the controller needs a concession from the NDPA.

The controller shall not store personal data longer than is necessary to carry out the purpose of the processing. If the personal data shall not thereafter be stored in pursuance of the Norwegian Archives Act or other legislation, they should be erased.

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- The Personal Data Act
- The Personal Data Regulation
- The Norwegian Working Environment Act

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

As a general rule, no. However, in certain circumstances, the court may disallow evidence that has been obtained in an improper manner.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

Under the Norwegian Working Environment Act, any undertaking that regularly employs at least 50 employees should provide information concerning issues of importance for the employees' working conditions, and discuss such issues with the employees' elected representatives. Likewise, the employer is obliged to discuss the needs, design, implementation, and major changes to control measures in the undertaking with the employees' elected representatives.

Under the Data Protection Authority, a company may designate an independent data protection officer, who would be responsible for ensuring that the employer complies with the Personal Data Act and relevant Regulations.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

As it currently appears, there will be no legal changes.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

Subject to the Data Protection Act, the NDPA may issue orders to the effect that violation of the provisions laid down in or pursuant to the Act shall result in a fine to the Treasury (Data Offence Fine). The NDPA may also impose a coercive fine, which will run for each day from the expiry of the time limit set for compliance with the order until the employer complies.

The employer may also be subject to compensate an employee for damages suffered as a result of processing the employee's personal data contrary to provisions laid down in or pursuant to the Act. This may include both actual financial loss and/or compensation for damages of a non-economic nature (compensation for non-pecuniary damage).

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

Subject to Norwegian employment law, incriminating photographs will typically qualify for termination of employment.

In addition, demeaning or insulting statements made on Facebook will usually result in further investigation of, e.g., the employee's position and the context of the statements.

This distinction of termination for cause or entitlement to severance is unfamiliar under Norwegian employment law. Instead, the relevant question is whether these such actions might call for dismissal with or without notice.

For more information about transferring personal data in Norway, please contact:

Nicolay Skarning
Kvale Advokatfirma DA
T: +47 22 47 97 00
ns@kvale.no
www.kvale.no

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

Under Polish law, the transfer of personal data to a third country outside the EU is authorised if the country of destination ensures an adequate level of protection. When that occurs, the transfer is considered as if conducted within the EU, and the general principles of the Polish Data Protection Act (DPA) must be observed.

If, however, the level of protection is considered inadequate, a transfer may still be allowed in particular cases, and shall be formalised inter alia by any of the following means: acquiring the formal consent of the Polish DPA (GIODO) confirming that the data controller ensures adopting adequate security measures for the protection of privacy, as well as the rights and freedoms of the persons whose personal data is to be transferred; obtaining written consent for such transfer granted by the persons whose personal data is to be transferred; drafting a contract based on the EC Standard Contractual Clauses for the transfer of personal data to third countries; drafting Binding Corporate Rules, which are then authorized by the Polish DPA (GIODO).

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

Such national authorisation is currently not required. The Polish DPA provisions have been amended in this regard, and are binding from the beginning of 2015.

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

Whistleblowing schemes are not regulated under Polish law, despite the Polish DPA (GIODO) recommendations provided to the Polish Ministry of Labour and Social Policy.

Note, however, that Article 29 Working Party has adopted an opinion on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, and banking and financial crime. The Polish DPA (GIODO) encourages entities that implement a whistleblowing system to comply with this opinion. Thus, subject to the foregoing, such whistleblowing reports shall be transferred within a multinational to a country outside the EEA observing the same data transferring principles as set forth above.

Once employees consent to introducing the whistleblowing hotline, there is no express obligation to obtain their consent for the transfer itself. This remains without prejudice to the requirement to notify the employees about the operation of the whistleblowing hotline, discouraging anonymous reports etc.

CONTENTS

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

There is no specific legislation regarding monitoring of employees. However, the following general laws and regulations apply:

- Article 8, European Convention on Human Rights, 1950
- The Polish Constitution
- The Labour Code of December 23, 1997
- Act on Protection of Personal Data of August 29, 1997
- Articles 23 and 24, the Polish Civil Code
- Regulation Regarding Health and Safety in the Workplace with Respect to Work Positions Equipped with Display Units (a regulation of the Ministry of Labour and Social Policy of December 1, 1998.)

Based on the foregoing, it has been established that monitoring of employees may be generally permitted as long as it is justified by the interests of the employer, is proportionate for the intended purposes, and does not violate employees' personal rights. The employer must notify employees that the workplace and/or IT infrastructure at their disposal will be monitored and also provide the employees with information regarding the scope and purpose of such control prior to its commencement.

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

Polish civil (employment) law does not recognize any doctrine restricting the use of unlawfully obtained evidence. However, an employer using such evidence in court would have to take into consideration the serious risk of being accused of violating the employee's personal rights and data protection regulations unless such pieces of evidence are collected in line with the foregoing rules on lawful monitoring of employees.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

According to Polish law, employers are obliged to inform Works Councils about and consult with them regarding actions that may cause significant changes in the organization of the workplace. The implementation of technology that allows monitoring may fall into this category since it affects all employees and the degree of the intervention in the employee's private sphere is significant. Thus, it is advisable to consult with the Works Council regarding such action if in fact one has been established in the particular workplace.

Further, if the regulations regarding monitoring are to be included in the working regulations (i.e., work rules), they must be agreed to by the enterprise trade union(s) (if applicable, and which may be established independently of the Works Councils), subject to particular provisions governing the operation of trade unions.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

Generally, no.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

The violation may lead to compensation for injury to the employee's privacy. Further, a complaint to the Polish DPA (GIODO) may be filed, which would trigger control proceedings.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

In general, under Polish law employees are allowed to express critical comments regarding their employer in line with the freedom of speech enjoyed thereby. However, the manner (i.e., form of expression) in which such critical comments are presented shall be adequate and balanced. It is also important that such critical comments do not result in work disorganization or impede the normal functioning of the workplace. It shall be assumed that all employees have a loyalty obligation towards their employer, and are bound to care about the welfare of the workplace.

Notwithstanding the foregoing, exceeding the boundaries of permissible criticism against the employer may provide justification for terminating the employment relationship with observance of the respective notice period. Dismissal (i.e., immediate termination) following criticism of the employer shall be deemed lawful in extraordinary scenarios.

Determining whether uploading incriminating photos of inappropriate behaviour at the workplace also constitutes cause for termination of the employment relationship (dismissal) shall be based on a case-by-case analysis of all the contributing factors. When conducting such a determination, it is important to establish whether the employee in question intended to harm the company (or its good name) and if the posting actually caused such harm. Further, it is also important to determine whether it is a one-time incident or the employee has repeatedly misused social media in a manner harmful or potentially harmful to the employer, and had previously been warned to cease such behaviour. The latter scenario might result in a lawful dismissal of the employee in question.

For more information about transferring personal data in Poland, please contact:

Andrzej Czopski
Miller Canfield, W. Babicki, A. Chełchowski and Partners
T: +48 58 782 0050
czopski@pl.millercanfield.com
www.millercanfield.pl

Magdalena Olkiewicz
Miller Canfield, W. Babicki, A. Chełchowski and Partners
T: +48 58 782 0050
olkiewicz@pl.millercanfield.com
www.millercanfield.pl

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

Under Portuguese law (Protection of Personal Data Law - Law no. 67/98, of 26 October), the transfer of personal data to countries outside the European Union can only occur if the processing of such data is lawful under the provisions of the Protection of Personal Data Law and the receiving country ensures an adequate level of protection. The adequacy of protection of recipient countries is assessed by the national authority for the protection of personal data (CNPD – *Comissão Nacional de Protecção de Dados*), which publishes a list of countries that are considered to meet its requirements and criteria.

Since the United States is not a part of this list, the transfer is subject to prior authorization by the CNPD, which may only be granted if:

- The data subject has given his/her consent unambiguously to the proposed transfer;
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request;
- The transfer is necessary for the performance of a contract concluded in the interest of the data subject between the controller and a third party;
- The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defence of legal claims;
- The transfer is necessary in order to protect the vital interests of the data subject; or
- The transfer is made from a register, which, according to laws or regulations, is intended to provide information to the public and is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

Notwithstanding, the CNPD may still authorise the transfer of data if the data controller establishes adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals, and as regards the exercise of the corresponding rights.

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

Yes. The CNPD authorises such a transfer under the pre-approved contractual clauses, without additional requirements.

Notwithstanding, the transfer must be subject to prior authorisation.

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

The transfer of whistle-blowing reports containing personal data to a country outside the European Union must be subject to prior authorisation by the CNPD in the terms set out above.

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- Labour Code (Law no. 7/2009, of 12 February); updated version
- Protection of Personal Data Law (Law no. 67/98, of 26 October); updated version

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

Yes. The Portuguese Constitution provides protection to all citizens regarding personal rights, including those related to one's private life, under article 26, paragraph 1. Moreover, pursuant to article 32, paragraph 8, evidence obtained through abusive intrusion into one's private life, correspondence, or telecommunications is deemed void. (Note: Although this provision is specific for criminal procedures, the courts have a history of extending its effects to disciplinary procedures against employees, given the analogous nature with criminal cases.)

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

Under Portuguese law, no such information/consultation/co-determination rights exist with regard to monitoring of employees.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

Although the text of the Regulation specifically authorises Member-States to legislate on this matter, we do not foresee any legal changes to the monitoring of employees provision. Notwithstanding, such may occur in the future.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

Employees may resort to general civil and criminal means to claim damages (pecuniary and moral) for violation of rights, namely for breach of correspondence or intrusion into one's private life.

The employer may also face administrative charges for unlawful data processing, some cases of which may also constitute a criminal offense.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

The issues surrounding dismissal of employees for such actions as posting incriminating photos and/or derogatory comments about an employer and/or other employees are quite sensitive, and must be analysed on a case-by-case basis, given the ever more difficult distinction between private and public life, as well as private and work life.

Although the subject has not been widely explored academically, the fact of the matter remains that the employee is bound to general duties of loyalty and respect towards his/her employer. It is all the more disciplinarily relevant when the behaviours on Facebook have an impact on the employer's business, even indirectly. What must be ascertained to assess disciplinary relevancy is the behaviour itself, and not particularly the medium.

A recent court decision (Acórdão do Tribunal da Relação do Porto, 8 September 2014, Process no. 101/13) ruled that a disciplinary termination based on behaviours on Facebook (specifically, derogatory comments made towards the board and co-workers) was lawful. The Court relied on the following factors for its case-by-case assessment:

- Type of social media and respective privacy parameters; regarding Facebook in particular, whether comments are made on a personal profile or a group page.
- Members of each social network, who can be actual "friends" or not even know each other.
- Account/page settings, in relation to access to content, for assessing its public or private nature and expectation of privacy.
- The number of "friends" or members of the group. In other words, the size and level of trust in which the information is being disseminated. (This led the Court to conclude the existence of a new sphere of privacy regarding certain behaviours, particularly due to social media – the semi-public.)
- Period of time the information is kept online and available.

The Court concluded for the lawfulness of the dismissal based on the following:

- The information was shared in a Facebook group, which given its characteristics, was outside the scope of the legal provisions regarding the employee's right to privacy.
- The group was of a professional nature. Company matters of interest to employees were debated; thus, there were a considerable number of members – all employees or former employees.
- The employer became aware of the behaviours (i.e., the derogatory comments made by the employee towards board members and co-workers) via members of the group on a platform where matters of a professional nature were discussed.
- The comments were mainly considered false, offensive, and detrimental to the employer, and therefore were a serious enough breach to be considered just cause for termination, as legally defined.

For more information about transferring personal data in Portugal, please contact:

César Sá Esteves
SRS Advogados
T: +351 21 313 20 00
cesar.esteves@srslegal.com
www.srslegal.pt

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

Under Swedish Law, personal data may be transferred to a third country in one of the following situations:

- If there is an adequate level of protection in the recipient country (not applicable in this case since Umpire is not Safe Harbour certified). Note: earlier this year, the European Court of Justice ruled: 1) that each data-protection authority may examine whether a transfer of data complies with European data protection rules; and 2) that the Safe Harbour Agreement itself is invalid (C-362-14). Our evaluation of the ruling is that it does not have an impact on the answers in this overview. However, when transferring data to the U.S., companies and data controllers that previously were able to rely on the Safe Harbour agreement now must comply with any of the other requirements stipulated in the Swedish Personal Data Act as described below. Furthermore, EU data protection authorities have, on 16 October 2015, released a statement in which they consider that Standard Contractual Clauses and Binding Corporate Rules (BCR) can be used until end of January 2016.
- If there are adequate safeguards with respect to the protection of the rights of the data subjects. Such safeguards may result from:
  - o Standard Contractual Clauses approved by the EU Commission;
  - o Binding Corporate Rules. These are rules that a multinational company group may have adopted in order to regulate its personal data processing.
- When the data subject has given his/her consent to the transfer. The consent must be freely given and refer to the transfer of personal data as such.
- In addition to consent, there are a few specific situations where personal data may be transferred, regardless of whether there is an adequate level of protection or other safeguards. These include if the transfer is necessary for the:
  - o performance of a contract between the registered person and the controller of personal data or the implementation of pre-contractual measures taken in response to the request of the registered;
  - o conclusion or performance of a contract between the controller of personal data and a third party that is in the interest of the registered person;
  - o establishment, exercise, or defence of legal claims; or
  - o protection of vital interests of the registered person.

CONTENTS

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

No, authorisation is not needed in Sweden. Nor is a specific notification (or submission of copies of the contract) required for transfers based on the Standard Contractual Clauses.

In principle, however, all personal data processing must be notified to The Data Protection Authority in Sweden. Even so, there are a great number of exemptions from this rule. For example, a controller who has appointed a data protection officer within the company does not have to notify the personal data processing. It would be appropriate, therefore, for the Swedish subsidiary to appoint such a person. Furthermore, certain kinds of processing operations that are not likely to lead to privacy infringement do not have to be notified.

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

It is possible for companies in Sweden to process personal data in a whistle-blowing system without having to apply for special permission from the Data Inspection Board. The local subsidiary (as the data controller) must nevertheless comply with all relevant provisions in the Swedish Personal Data Act when processing personal data in the whistle-blowing system. With respect to transferring the whistle-blowing reports, the general conditions described in the first question above are therefore applicable.

The easiest options for the multinational would most likely be to use EU Standard Contractual Clauses or to adopt Binding Corporate Rules. However, a controller who wants to adopt Binding Corporate Rules must apply to The Data Protection Authority for an exemption from the principal ban on such transfers.

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- Personal Data Act
- Personal Data Ordinance
- Camera Surveillance Act
- Swedish Criminal Code
- European Convention on Human Rights

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

Generally, no. According to the Swedish Code of Judicial Procedure, the court shall, after evaluating everything that has occurred, determine what has been proven in the case. In other words, the principal rule entails that any proof, without limitations, can be presented before the court, which is not bound by any regulations when determining the value of an item of evidence. The Swedish legal system does not prescribe that it is forbidden to present evidence that was obtained while breaking the law. Nor is the court prevented from ascribing such proof to be of great value.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

The Act on Co-Determination at Work contains rules on information and negotiation that imply a duty for the employer to negotiate with the union organisation before the employer decides to monitor or supervise employees. Furthermore, according to general information obligations of the employer, the union organization is entitled to continuous insight into the business of the employer.

The Working Environment Act stipulates that Employee Representatives are entitled to consult documentation and obtain any other information needed for their activities. Representatives, through committees, are also entitled to participate in the planning of new or changed work processes, working methods, and the re-organisation of the work place.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

In principle, no. However, the higher fines and generally stricter requirements will have an overall impact on the legal landscape of employers' data processing.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

In case of intentional or, by gross negligence, illegal use of personal data, the employer may be sentenced to fines – or corporate fines, in some cases – or imprisonment of at most six months. If the offence is grave, the penalty is at most two years' imprisonment.

The employer may also have to compensate the registered person for damages and violation of personal integrity caused by the processing of personal data.

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

In Sweden, employees have a duty of loyalty towards their employer. This duty is continuous during the entire period of employment, both during work and at leisure, and involves, inter alia, an obligation to follow the employer's work management decisions and polices, which could include social media use. Of particular interest to the issue of social media use is that the duty of loyalty includes professional secrecy, which entails that an employee is not allowed to abuse the otherwise statutory right to criticize the employer. This applies to social media, as well as other forms of communication.

Breach of the duty of loyalty may constitute grounds for dismissal, depending on the severity of the inappropriate behavior. Although dismissal typically requires prior warning to the employee, if the inappropriate behavior is of such severity that the employer cannot reasonably be expected to continue the employment relationship, a prior warning is not necessary.

Regardless of the above, the main rule under the Swedish Personal Data Act is that an employer is not allowed to read employees' private e-mails or monitor their social media activities. It may, however, be allowed in an individual case, e.g., if an employer has a justified interest to get access to certain personal data that outweighs the employee's interest of integrity. The employee's right to full privacy or not must be decided after an assessment of the circumstances on a case-by-case basis.

For more information about transferring personal data in Sweden, please contact:

Olle Linden
Vinge
T: +46 (0)10 614 15 44
olle.linden@vinge.se
www.vinge.se

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

According to the Swiss Federal Act on Data Protection (FADP), a transfer of personal data of employees out of Switzerland is only lawful if the personal rights of the data subject are not seriously threatened by the transfer. In particular, a transfer is deemed to imperil the personal rights of the data subject if the country to which the data is transferred does not guarantee an adequate level of protection.

A transfer of data from Switzerland to a country without adequate protection is still possible, but it is required to meet one of the specific exceptions for data transfer abroad listed in Article 6 para. 2 FADP.

The U.S.-Swiss Safe Harbor Framework Agreement (Safe Harbor), which is identical to the U.S.-EU Safe Harbor Framework, is one of the specific exceptions under Article 6 para. 2 FADP for the transfer of data. Under this Agreement, entities or organizations register and commit themselves ("self-certification") to comply with the principles of data protection provided in the Safe Harbor.

Once an entity is self-certified, no further authorisation is required to transfer personal data to the U.S.

However, following the decision of the European Court of Justice ruling on October 6, 2015 that the U.S.-EU Safe Harbor Framework was invalid, Swiss authorities are currently questioning the perpetuation of the U.S.-Swiss Agreement. At this stage, the Swiss authorities – through the Swiss Data Protection Commissioner (FDPIC) – recommend using data transfer agreements for data transfers to U.S. recipients. FDPIC requires that these additional agreements regulate the following points:

- A duty on the data transferor and transferee to inform affected data subjects in a clear and comprehensive manner about potential interception by U.S. authorities so that the data subjects can exercise their rights.
- An undertaking from the data transferor and transferee to provide the affected data subjects with the necessary means for protecting their rights, to carry out the corresponding procedures, and to accept the resultant decision.

In the case of a non-certified Safe Harbour entity (such as Umpire), the data may still be transferred if the data subject has agreed to the transfer in the specific case, or if the disclosure is made within the same legal person or company or between persons or companies under the same management, provided that those involved are subject to data protection rules that ensure an adequate level of protection. In the latter case, the Federal Data Protection and Information Commissioner must be informed of the data protection rules.

CONTENTS

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

Exceptions for data transfer from Switzerland to a country without adequate protection are listed in Article 6 para. 2 FADP. The use of contractual clauses ensuring an adequate level of protection, such as the EU Standard Contractual Clauses, constitutes one of these exceptions. No further authorisation is necessary for the transfer.

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

Swiss law does not specifically regulate whistle-blowing within the private sector. The rules outlined above also apply to the transfer of whistle-blowing reports containing personal data.

According to current Swiss law, an employee is not authorized to provide information to third parties if such information could adversely affect his/her employer, unless higher interests are at stake.

However, a bill is being debated in the Swiss parliament that aims to regulate and protect whistle-blowers through a three-step procedure: the employee would have to alert his/her employer in case of wrongdoings. In the event the employer does not remedy the deficiencies, the employee may then transfer the information to the authorities or as a last resort to the public. Alternatively, the employer can set up an internal reporting system.

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- Title 10 of Swiss Code of Obligations
- Swiss Federal Act on Data Protection
- Swiss Criminal Code
- Swiss Federal Labour Law
- The Regulation 3 relating to the Swiss Federal Labour Law

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

In general, evidence gathered unlawfully is prohibited and not binding in Courts. However, the judge may, at his/her discretion, consider the evidence admissible if public interest is deemed overriding.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

Employers must notify their employees in advance in a clear and plain manner about the monitoring. Employees must be involved in the planning, installation, and operation of the monitoring system. Furthermore, the employer shall obtain an employee's consent before consulting his/her private data carrier, or it must have suspicion based on factual indications that an employee has taken part in unlawful activities. Vague impressions or the lack of trust in the employee do not constitute sufficient factual indications.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

Since Switzerland is not a member of the European Union, EU regulations are not directly applicable. Therefore, the upcoming EU data privacy shall not change the legal landscape regarding monitoring of employees. Nevertheless, Swiss authorities remain attentive to the European legislation changes.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

In case of unlawful monitoring of employees, the employer faces civil, administrative, and criminal sanctions. The employer can be ordered to compensate an employee for moral damage as a result of infringing the employee's personal rights due to the unlawful monitoring. As for criminal charges, employers can be subject to sanctions ranging from monetary penalties (for opening private mail in order to acquaint themselves with its contents) to a deprivation of liberty up to three years (for monitoring and recording conversations without the parties' consent).

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

Swiss law does not specifically regulate employee's use of social media. Such use falls under the employees' general duty of care and loyalty inherent in any employment contract. According to this duty, the employee must carry out the work assigned to him with due care and loyally safeguard the employer's legitimate interest. The duty of loyalty implies that the employee refrains from criticizing his superiors or the company strategy, or from acting inappropriately. Moreover, insult or derogatory comments (posted on social media or said face to face) constitute an infringement of personality rights.

It should be noted that in Switzerland, the principle of contractual freedom prevails and either party is free to terminate the employment contract by observing the applicable notice period. This being said, both the infringement of personality rights and the breach of the duty of loyalty may constitute a valid reason justifying a summary dismissal, i.e., without notice and with immediate effect. The law defines such valid reason as being any circumstance under which the terminating party cannot be expected in good faith to continue the employment relationship even during the notice period. The court decides, in its own discretion, whether, given the circumstances of the individual case, the contentious issue sets a sufficient basis for the immediate termination of the employment relationship. According to case law, only a particularly serious offence may justify a summary dismissal.

For more information about transferring personal data in Switzerland, please contact:

Vibeke Jaggi
Froriep
T: +41 22 839 63 00
vjaggi@froriep.ch
www.froriep.com

Roland Kaufmann
Froriep
T: +41 22 839 63 00
rkaufmann@froriep.ch
www.froriep.com

Transfer of Personal Data of Employees Outside of the European Economic Area

(See page 4 for the hypothetical upon which these responses are based.)

QUESTION: Under what conditions is the transfer of personal data by the local subsidiary to the parent company located in a country outside the European Economic Area (EEA) lawful under national law?

The Data Protection Act 1998 (DPA) allows for the transfer of personal data outside of the EEA only where the receiving country or territory is deemed to have an adequate level of data protection.

In those instances where a country or territory is not deemed to have adequate protection, the parties can themselves assess whether the level of data protection is adequate in all circumstances. The UK regulator of the DPA, the Information Commissioner's Office (ICO), has produced guidance on this. Part of assessing whether the level of protection is adequate in all the circumstances involves considering whether one of the statutory exemptions shall apply.

Please be aware that the Court of Justice of the European Union (CJEU) recently (October 2015) declared the EU – U.S. Safe Harbour regime to be invalid. Before the CJEU decision, "Safe Harbour certification" meant that a company in Europe could rely on the U.S. company's Safe Harbour certification as providing a sufficient legal basis for transferring personal data to the U.S. company. That legal justification has been removed with immediate effect, and those European companies will be required to look at alternative legal structures, for example, individual consent or "Model Contracts" approved by the European Commission instead of reliance on Safe Harbour certification.

This decision has created considerable uncertainty for companies and organisations that have relied on "Safe Harbour certification" and it is hoped that data protection authorities, such as the UK Information Commissioner will provide clarification in due course.

CONTENTS

QUESTION: When using the EU Standard Contractual Clauses, does Umpire still need a national authorisation to proceed with the transfer? If so, under what conditions is authorisation granted?

The use of the EU Standard Contractual Clauses is an exemption to the DPA, and can be used where a transfer is being made to a country or territory with inadequate data protection. If the Standard Clauses are amended, ICO approval should be sought; otherwise no authorisation is required.

QUESTION: Under what conditions are local subsidiaries allowed to transfer whistle-blowing reports containing personal data within a multinational to a country outside the EEA?

The DPA requires that personal data cannot be processed unless at least one statutory condition is met. One such condition is that the processing is for a legitimate purpose by the data controller (Umpire's subsidiary), unless the processing is unwarranted by reason of prejudice to the rights or legitimate interests of the data subject. The ICO recommends that any such analysis is documented in a Privacy Impact Assessment (PIA) to demonstrate that due consideration has been given to ensure there is adequate protection.

The ICO has not commented specifically on the transfer of whistle-blowing reports outside of the EU within a multinational corporate group. On transfers of personal data within a corporate group, it suggests that the group should consider seeking authorisation under the Binding Corporate Rules (BCRs), which would allow it to transfer personal data throughout the company, including to entities outside of the EEA. However, the process for gaining certification for BCRs can be resource-intensive.

Monitoring of Employees

QUESTION: What are the relevant laws concerning monitoring of employees at work – both off- and online?

- The Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

QUESTION: If evidence of misconduct or breach of contractual duties is gathered by monitoring, is there something comparable to the U.S. "Fruit of the Poisonous Tree Doctrine" (i.e., evidence gathered illegally cannot be presented in court in dismissal cases)?

Generally, an employment tribunal will decide on a case-by-case basis whether or not to consider evidence gathered by monitoring. However, it has been held that the employer's use of a private investigator to take covert footage of an employee during working hours was not disproportionate or unreasonable in the circumstances where it was found that the employee was acting fraudulently in a public place.

The ICO's Employment Practices Code states that a PIA should be carried out before undertaking any employee monitoring. A tribunal found that, because the employer had not followed this Code, it was unfair to rely on this footage in making the dismissal. However, as the ICO's Codes do not have statutory effect, there is no legal obligation on the part of the employer to follow the guidance, although it would be recommended.

QUESTION: What type and scope of information/consultation/co-determination rights exist for employee representatives in connection with monitoring of employees?

Employers do not have to notify employees when they intend to carry out covert monitoring. However, taking such action is generally considered permissible only where the justification for such monitoring sufficiently outweighs the employee's privacy rights. The ICO recommends that a PIA be carried out in advance of any monitoring – particularly for covert monitoring – but there are no enhanced rights with respect to employee representatives, and there is no express duty to consult with employee representatives about monitoring.

QUESTION: Will the upcoming EU data privacy/data protection regulation change the legal landscape when it comes to monitoring of employees?

Although recommended by the ICO, there currently is no legal obligation for employers to carry out a PIA before undertaking monitoring of employees. However, this is likely to change upon the introduction of the upcoming EC Data Protection Regulation, which, in its current draft form is set to make PIAs mandatory throughout Europe.

QUESTION: What damages/remedies do employers face in case of illegal monitoring of employees?

The DPA provides that an individual is entitled to compensation if he/she suffers damage or distress as a result of a breach of the DPA by a data controller. This is by way of a claim through the courts rather than to the ICO. However, in cases of illegal monitoring, the ICO is entitled to fine a data controller up to £500,000 for breaches of the DPA.

In the event of a successful claim for unfair dismissal arising from an unfair or unlawful investigation, the employee could also be awarded compensation from the employment tribunal up to a statutory maximum, which is currently £78,335 in Great Britain (£78,400 in Northern Ireland).

Use of Social Media

QUESTION: Can an employee be dismissed for cause if he or she uploads to Facebook incriminating photos of inappropriate behaviour at the workplace and/or for posting on Facebook or other social media insulting or derogatory comments about the employer and/or other employees?

Photographs uploaded to Facebook or other social media that provide clear evidence of potential gross misconduct, especially if the identity of the offending employee is apparent, will require an internal disciplinary investigation. The photos and any other postings will be vital evidence for a disciplinary hearing.

It is important, however, for employers to follow a fair process of investigation, disciplinary hearing, and appeal to avoid the risk of a subsequent unfair dismissal claim. The objective will be to find a reasonable belief of what occurred. If the employee is found to have committed any acts of gross misconduct as evidenced in the Facebook posts, he/she would be dismissed with immediate effect and have no right to any notice or severance pay.

Likewise, an employee who posts insulting or disparaging comments on Facebook – including those relating to discrimination/harassment, as well as any protected characteristic (e.g., gender, sexual orientation or race) – could also face dismissal for gross misconduct, with no severance pay. Mitigating circumstances may also come into play, which would need to be tested in a disciplinary hearing, and the way in which the employee responds may inform the reasonable response from the employer.

The UK courts and tribunals have developed the following trends with regard to disciplinary cases involving employee abuse of social media: employees should have no reasonable expectation of privacy when posting to social media; an employer must prove reputational damage; and it is vital for employers to have a social media policy in place that clearly sets out the expected standards of behaviour and warns employees that their conduct on social media could result in disciplinary action up to dismissal for gross misconduct for breach of policy.

For more information about transferring personal data in the UK,* please contact:

Scotland:
David Morgan
Burness Paull
T: +44 (0)141 273 6770
david.morgan@burnesspaull.com
www.burnesspaull.com

England:
Michael Leftley
Addleshaw Goddard
T: +44 020 7788 5079
michael.leftley@addleshawgoddard.com
www.addleshawgoddard.com

Richard Yeomans
Addleshaw Goddard
T: +44 020 7788 5351
richard.yeomans@addleshawgoddard.com
www.addleshawgoddard.com

Northern Ireland:
Gareth Walls
A&L Goodbody
T: +44 28 9031 4466
gwalls@algoodbody.com
www.algoodbody.com

**This overview was prepared by Burness Paull on behalf of the three ELA member jurisdictions in the UK – England, Northern Ireland, and Scotland.*

PARTICIPATING ELA MEMBER LAW FIRMS

ALBANIA
Renata Leka
Boga & Associates
Ibrahim Rugova Str., P.O. Box 8264
Tirana, Albania
T: +355 4 2251 050
rleka@bogalaw.com
www.bogalaw.com

AUSTRIA
Hans Kristoferitsch
CHSH Cerha Hempel Spiegelfeld Hlawati
Partnerschaft von Rechtsanwälten
A-1010 Vienna, Parkring 2, Austria
T: +43 1 514 35-191
hans.kristoferitsch@chsh.com
www.chsh.com

BELGIUM
Jan Hofkens or Isabel Plets
Lydian
Tour & Taxis
Avenue du Port 86c Havenlaan
Box 113
Brussels, 1000 Belgium
T: +32 (2) 787 90 37 (Jan)
T: +32 (2) 787 90 83 (Isabel)
jan.hofkens@lydian.be
isabel.plats@lydian.be
www.lydian.be

BULGARIA
Vesela Kabatliyska
Dinova Rusev & Partners Law Office
22 Emile de Laveleye Street
1000 Sofia, Bulgaria
T: +359 (0)2 903 01 01
vesela.kabatliyska@drp-legal.com
www.drp-legal.com

CROATIA
Hrvoje Vidan
Vidan Law Office
Preradoviceva 10
10 000 Zagreb, Croatia
T: +385 1 4854 070
hrvoje.vidan@vidan-law.hr
www.vidan-law.hr

CYPRUS
Nicholas Ktenas
Andreas Neocleous & Co LLC
5 Lemesou Ave, 2nd Floor
2112 Aglantzia
Nicosia, Cyprus
T: +357 22 110324
ktenasn@neocleous.com
www.neocleous.com

CZECH REPUBLIC
Sasha Stepanova
Kocian Solc Balastik
Jungmannova 745/24
110 00 Prague 1
Czech Republic
T: +420 224 103 316
sstepanova@ksb.cz
www.ksb.cz

DENMARK
Michael Hopp
Plesner
Amerika Plads 37,
2100 Copenhagen, Denmark
T: +45 36 94 13 06
mho@plesner.com
www.plesner.com

FINLAND
Anu Waaralinna or Sanna Alku
Castren & Snellman
P.O. Box 233 (Eteläesplanadi 14)
Helsinki, FI-00131 Finland
T: +358 (0) 20 7765 372 (Anu)
T: +358 (0) 20 7765 392 (Sanna)
anu.waaralinna@castren.fi
sanna.alku@castren.fi
www.castren.fi

FRANCE
Sophie Pélicier Loevenbruck
Fromont Briens
5/7 avenue du Coq, BP 80502
F-75421 Paris cedex 09, France
T : +33 (0)1 44 51 63 80
sophie.pelicier@fromont-briens.com
www.fromont-briens.com

GERMANY
Jan Tibor Lelley
Buse Heberer Fromm
Bockenheimer Landstrasse 101,
60325 Frankfurt am Main, Germany
T: +49 (0) 69 989 7235 0
lelley@buse.de
www.buse.de

GREECE
Effie Mitsopoulou
KYRIAKIDES GEORGOPOULOS LAW FIRM
28, Dimitriou Soutsou Str.
115 21, Athens, Greece
T: +30 210 817 1500
e.mitsopoulou@kglawfirm.gr
kg.law@kglawfirm.gr
www.kglawfirm.gr

IRELAND
Duncan Inverarity
A&L Goodbody
International Financial Services Centre
North Wall Quay
Dublin 1, Ireland
T: +353 1 649 2401
dinverarity@algoodbody.com
www.algoodbody.com

ITALY
Angelo Zambelli or Silva Annovazzi
Grimaldi Studio Legale
Via F.lli Gabba, 4, 20121 Milan, Italy
T: +39 02 3030 9390 (Angelo)
T: +39 02 3030 9303 (Silva)
azambelli@grimaldilex.com
sannovazzi@grimaldilex.com
www.grimaldilex.com

LUXEMBOURG
Louis Berns, Héloïse Bock or Philippe Schmit
Arendt & Medernach SA
41A, avenue J.F. Kennedy
L-2082 Luxembourg
T: +352 40 78 78 240 (Louis)
T: +352 40 78 78 321 (Héloïse)
T: +352 40 78 78 393 (Philippe)
louis.berns@arendt.com
heloise.bock@arendt.com
philippe.schmit@arendt.com
www.arendt.com

(continued)

PARTICIPATING ELA MEMBER LAW FIRMS

MALTA

Andrew J. Zammit, Ann M. Bugeja or Angela Bruno
CSB Advocates
The Penthouse Tower
Tower Business Center
Tower Street
Swatar, BKR 4013, Malta
T: +356 2557 2300
ajz@csb-advocates.com
amb@csb-advocates.com
abr@csb-advocates.com
www.csb-advocates.com

NORWAY

Nicolay Skarning
Kvale Advokatfirma DA
Fridtjof Nansens plass 4, 6th floor
PO Box 1752 Vika, 0122
Oslo, Norway
T: +47 22 47 97 00
ns@kvale.no
www.kvale.no

POLAND

Andrzej Czopski or Magdalena Olkiewicz
Miller Canfield, W. Babicki, A. Chełchowski and Partners
ul. Batorego 28-32
PL 81-366 Gdynia, Poland
T: +48 58 782 0050
czopski@pl.millercanfield.com
olkiewicz@pl.millercanfield.com
www.millercanfield.pl

PORTUGAL

César Sá Esteves
SRS Advogados
Rua D. Francisco Manuel de Melo, 21
Lisboa, 1070-085
Portugal
T: +351 21 313 20 00
cesar.esteves@srslegal.com
www.srslegal.pt

SWEDEN

Olle Linden
Vinge
Nordstadstorget 6
Box 11025
404 21 Göteborg, Sweden
T: +46 (0)10 614 15 44
olle.linden@vinge.se
www.vinge.se

SWITZERLAND

Vibeke Jaggi or Roland Kauffman
Froriep
4, Rue Charles-Bonnet
P.O. Box 399
1211 Geneva 12
Switzerland
T: +41 22 839 63 00
vjaggi@froriep.ch
rkaufmann@froriep.ch
www.froriep.com

UNITED KINGDOM

Scotland:
David Morgan
Burness Paull
120 Bothwell Street
Glasgow, Scotland
G2 7JL United Kingdom
T: +44 (0)141 273 6770
david.morgan@burnesspaull.com
www.burnesspaull.com

England:
Michael Leftley or Richard Yeomans
Addleshaw Goddard
Milton Gate
60 Chiswell Street
London EC1Y 4AG, England
T: +44 020 7788 5079 (Michael)
T: +44 020 7788 5351 (Richard)
michael.leftley@addleshawgoddard.com
richard.yeomans@addleshawgoddard.com
www.addleshawgoddard.com

Northern Ireland:
Gareth Walls
A&L Goodbody
6th Floor, 42-46 Fountain Street
Belfast BT1 5EF, Northern Ireland
T: +44 28 9072 7402
gwalls@algoodbody.com
www.algoodbody.com

www.employmentlawalliance.com