A deep dive into data processing at work: DPA advice on GDPR

Laurie-Anne Ancenys of Allen & Overy LLP looks at the recently adopted DPA guidance, which states that employers are unlikely to be able to rely on employee consent in the future.

The EU Article 29 Working Party's Opinion 2/2017, adopted on 8 June 2017[1], makes a new assessment of the balance between legitimate interests of employers and privacy expectations of employees and highlights the challenges brought by rapidly-evolving new technologies.

Since the last Opinions published on this topic in 2001 and 2002 by the Article 29 Working Party (WP29)[2], the use of sophisticated technologies by employers has resulted in more systematic processing of employees' personal data, raising concerns about the need to protect the private life of employees. The WP29's Opinion highlights the risks presented by new information technologies in a work environment and outlines practical recommendations for employers to protect their employees' rights to privacy by reference to scenarios.

New technologies may potentially turn into unjustifiable and invasive data processing at work. The use of online services (e.g. social media) or location data from a smart device is less visible to employees and the boundaries between home and work have become blurred. Therefore, it is likely to be difficult for employers to assess when monitoring may become intrusive by extending it to a private context. Monitoring technologies may be perceived by employees as putting more pressure on them. Nevertheless, with cyber-attacks on the increase, employers need to expand the level of data security and this, combined with the development of attractive cost-efficient IT tools, make the topic a matter of concern to all companies.

In its Opinion, the WP29 looks at obligations of data controllers under both the EU Data Protection Directive and the EU General Data Protection Regulation (GDPR). The scope is broad since it covers all types of employment relationships, regardless of whether or not the relationship is based on an employment contract.

A FOCUS ON KEY PRINCIPLES FOR EMPLOYERS

The WP29 starts its assessment by reinforcing that the importance of the key data protection principles, already in the Data Protection Directive, has been strengthened by the fast development of technologies at work.

The DPAs say the dependency that results from the employer/employee relationship means that consent is very unlikely to be a valid legal basis for data processing at work due to the power imbalance resulting from the employment relationship. Indeed, an employee's consent is unlikely to be freely given, revocable, specific and informed. The WP29 takes the example of default settings on devices that cannot reasonably rely on consent if no action is taken by the employee.

The performance of a contract and the legal obligations imposed on the employer may be invoked as valid grounds for data processing in an employment context. However, employers often rely on the legitimate interests ground in which case tighter precautions should be taken. In particular, the technology chosen should be necessary for the data processing, the least intrusive possible and proportionate to business needs. Monitoring should be implemented in a way that limits the geographical scope of the data processing, the types of data being processed and the specific periods of time during which the

processing is taking place.

Whatever the legal basis for data processing, the WP29 points out that a proportionality test should be conducted prior to data processing in order to assess its necessity to achieve a legitimate purpose as well as to identify the measures that should be put in place to minimise the extent of infringements of the rights to private life and secrecy of communications.

Finally, the WP29 highlights that, except in specific situations, decisions may not be taken by an employer based on automated processing when such decisions may have legal effects for employees or otherwise significantly affect them.

New concepts to be deployed with GDPR implementation

With the GDPR, new concepts such as Privacy by Design must be considered by employers when deciding to roll out tracking technologies. This means that the less invasive default settings should be proposed to employees when offering tracking tools. The principle of data minimisation should also be taken into account by employers.

Similarly, Data Privacy Impact Assessments (DPIA) must be conducted by employers where the processing may be considered as presenting high risks to the privacy of employees. Where the DPIA results show that risks cannot be sufficiently handled by the data controller, it must consult the relevant Data Protection Authority prior to the start of the processing.

The Opinion also highlights that Article 88 of the GDPR allows Member States to provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context. This may typically concern health and safety at work, protection of an employer's or customer's property or termination of the employment relationship. It will be interesting to see what specific areas of the employment relationship national legislators are willing to regulate. We assume that the French legislator is likely to take a position in a number of areas, but it appears that the DPAs are still unclear as to how national legislators will use the derogations.

Practical recommendations

Now that we are moving into an "all-digital" world, all employers should treat traffic data as enjoying the same fundamental rights and protections as so-called "analogue communications". Employers should adapt their mindset; transparency, proportionality and data minimisation must be the number one priority when implementing these new technologies.

Key practical recommendations, depending on the technology that is rolled out, include:

- **Tracking employees' location:** This might, for example, be done through tracking mobile devices, wearables, and controlling access to premises. In practice, such location tracking tools should be designed solely to track what is required for a legitimate purpose, and an option to turn them off should be offered where appropriate (in light of the circumstances). Other tools may also be set up to only share part of the data with the employer, or to share it only in very limited circumstances such as where a device is reported as lost.
- **Monitoring of vehicles used by employees:** Special care should be taken in relation to the use of technologies that may enable continuous monitoring both of the vehicle and of the driver (e.g. event data recorders). Where private use of the vehicle is allowed, the employee should in principle have the option to temporarily turn off the location tracking system, and the employer must ensure that the data collected is not used for illegitimate further processing. Clear information that employees' movements are being recorded shall be given to the employees, preferably displayed prominently in every car. Proportionality of the data processing shall be ensured, meaning that monitoring outside of working hours is unlikely to be legitimate unless a justifiable necessity exists. The useful examples provided should be read in conjunction with previous Opinions on this topic[3].
- **Bring Your Own Device (BYOD):** In order to prevent monitoring of private information, appropriate measures must be in place to distinguish between private and business use of the device. Methods should also be implemented to ensure that data is securely transferred between the device and the network.
- **Monitoring of remote working:** While technical security measures must be implemented by the employer to prevent unauthorised access, loss or destruction of information, software packages now widely offered by IT service providers should, likewise, only be deployed when proportionate and non-excessive data processing can be ensured in light of the risks presented by home and remote working.
- **Video monitoring systems:** Attention must be paid to video analytics that allow monitoring of workers' facial expressions. Such technologies are unlikely to be seen as lawful, respectful of rights and freedoms of employees and proportionate to business needs. The data processing of such video systems is also likely to amount to profiling and to decisions made on automated processing. A Data Protection Impact Assessment (DPIA) may have to be conducted and documented before implementing such systems.
- **Monitoring of ICT use:** The Opinion clearly leaves open the possibility of deploying solutions that monitor employee ICT usage, subject to proportionality and transparency. There should be limits on monitoring, such as the exclusion of personal files / communication and traffic where interception endangers the appropriate balance of rights. Employers should not keep permanent logs of employee activity but if required, systems should be configured not to store data unless an incident occurs. As good practice, employers could offer alternative unmonitored access for employees. Web filters would seem to be the most appropriate way to monitor Internet usage at work since "all-day" Internet monitoring is prohibited by law in many EU jurisdictions.
- **Social media:** Checking job applicants' social media profiles is only

permitted where necessary and relevant to the role being applied for, where information is publicly available and where they have been informed about this beforehand. Employers should refrain from requiring an employee or a job applicant to give access to information that he or she shares with others on social media. If an employer uses social media, employees should always have the option to use a non-work related profile. This should be specified in the company's IT or social media policy and in the employment contract.

- **Cloud services:** Cloud solutions should enable employees to set their own private space which the employer cannot access. The usual compliance mechanisms offered for international data transfers should be implemented whenever personal data is transferred outside of the EU to a country not providing an adequate level of protection. The mechanisms should be chosen in light of the already implemented data transfer solutions whenever feasible.

Effective, transparent information must be given to employees about new technologies and any monitoring that is taking place. For all of the above listed uses of new technologies, it is highly recommended that employers implement clear and easily accessible rules and policies demonstrating that the monitoring in place is legitimate and proportionate to their business requirements. These policies should explain the rules that apply to different types of monitoring tools. Policies should be reviewed annually to assess whether less invasive methods could be used. Data retention is also a critical topic to address.

The WP29 recommends involving a "representative sample of employees" in the development and evaluation of such rules and policies given their potential to infringe on employees' privacy rights. Employers should consider putting in place a separate advisory group to perform this role, aside from any separate legal obligation that they may have under local laws to inform, consult or seek the approval of any works council or other representative body. French law already requires employers to inform and consult the employees' representatives with regard to implementation of such policies.

Appropriate communication to employees is also recommended to ensure they are all well aware of their responsibilities in the use of IT tools, e.g. when setting up or switching parameters. Training sessions would be seen as good practice in case of conflicts.

Comment

Overall, in its Opinion, the WP29 reinforces the view that prevention is a far safer approach than detection. Although it does not say anything significantly new, it is a reminder to employers to think carefully about whether, why, and how, to conduct monitoring rather than doing so systematically, in spite of the new technologies at their fingertips. The Opinion is not binding law but does reflect the views of national regulators on how the law should be interpreted; its guidance will therefore be influential both in the short-term and in the GDPR world.

AUTHOR

Laurie-Anne Ancenys is a Counsel in the Corporate Department (IT), Allen & Overy LLP, Paris. Email: Laurie-Anne.Ancenys@AllenOvery.com

REFERENCES

1 ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
2 WP29, Opinion 08/2001 on the processing of personal data in the employment context, WP48, 13 September 2001; and WP29, Working document on the surveillance of electronic communications in the workplace, WP55, 29 May 2002.
3 WP29 Opinion 13/2011 on Geolocation services on smart devices, WP 185, 16 May 2011; and WP29, Opinion 5/2005 on the use of location data with a view to providing value-added services, WP 115, 25 November 2005.

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Russia increases DPA's powers and fines

Since 1 July, companies in Russia face increased fines and its DPA, *Roskomnadzor*, can prosecute more offences. **Stewart and Merrill Dresner** report from St. Petersburg.

Victor Naumov, Partner, and Head of IT/IP and telecommunications law, and Dentons' Managing Partner in St. Petersburg, explained that the data protection issues faced by the firm's clients, leading and high-profile global Internet companies, are often one of a group of legal issues including copyright and other aspects of intellectual property law. For example, the definition of personal data may now be applied, depending on circumstances to a set of technical

Continued on p.3

Ireland's DP Commissioner optimistic on One-Stop-Shop

At the *Privacy Laws & Business* 30th Anniversary International Conference, Helen Dixon, Ireland's Data Protection Commissioner, heralded a "new era" under the GDPR. **Oliver Butler** reports.

Dixon said that the GDPR is already having important effects on compliance and the development of capability. "Big companies are changing their behaviours and are advising smaller ones free of charge, and many larger companies are appointing DPOs, not necessarily with a legal background."

Dixon highlighted how accountability and regulatory conversations between data protection authorities

Continued on p.5

Issue 148 **August 2017**

INTERNATIONAL report

ISSUE NO 148 AUGUST 2017

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan.thomas@privacylaws.com

CONTRIBUTORS
Laurie-Anne Ancenys
Allen & Overy LLP, France

Paul Lavery
McCann FitzGerald, Ireland

Dr. Andrea Klára Soós
Andrea Klára Soós Law Office, Hungary

Odvar Bjerkholt
PL&B Correspondent

Oliver Butler
PL&B Correspondent

Patricia Gelabert
PL&B Correspondent

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

Look out for Russia's new enforcement powers

New data protection enforcement provisions took effect in Russia on 1 July. Now the DPA no longer needs to involve the state prosecutors, which makes the regime much more flexible (p.1). The DPA may also exercise its powers to block access to a website which is exactly what it did to LinkedIn. Russia is one of the 47 countries which are members of Council of Europe Convention 108. Professor Graham Greenleaf, *PL&B* Asia-Pacific Editor analyses the Convention's status and the potential for many more countries to join this club (p.12).

Slow progress is being made with GDPR national implementation laws. Germany adopted its law on 5 July and the Spanish Cabinet has been presented with a report on a DP implementation bill. The Director of Spain's Agencia told PL&B's conference that Spain is the first European DPA to create a certification scheme for DPOs (p.8).

Hong Kong is following Japan by introducing a public apology as a way to remedy a data protection problem (p.32). An early apology can often defuse a situation before formal enforcement is necessary.
In India, the courts have been debating whether privacy is a fundamental right under the constitution. The decision may re-set everything to do with privacy in India, says Graham Greenleaf (p.28).

The EU DPAs have issued GDPR Guidance on Data Processing at Work (p.16). The guidance largely follows the DPAs' previous thinking on the subject but has been updated with regard to new technologies. Technology was also an issue debated in May at the ethics event, which I attended, organised by the European Data Protection Supervisor and the ethics advisory group. Sometimes ethics helps, and sometimes it hinders privacy, see p.33.

As we finalise this edition, we await the court decision which could determine the use of EU model Contractual Clauses for EU-US transfers. Read about how we ended up in this situation, and about prospects for the future on p.7.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 100+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

3. E-Mail Updates
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues
Access all the *PL&B International Report* back issues since 1987.

5. Special Reports
Access *PL&B* special reports on Data Privacy Laws in 100+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Global Data Protection Officer, Denstu Aegis Network**"

Subscription Fees

Single User Access

International Edition **£550 + VAT***

UK Edition **£440 + VAT***

UK & International Combined Edition **£880 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-10 users. Enterprise licence for 11+ users.

Subscription Discounts

Introductory 50% discount. Use code HPSUB (first year only) for DPAs, public sector, charities, academic institutions and small and medium companies.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.
www.privacylaws.com/UK