# France's DPA imposes first sanction as Lead Authority

The CNIL has imposed a €250,000 fine on an online retailer for GDPR infringements in cooperation with other EU supervisory authorities. **Myria Saarinen** and **Charlotte Guerin** of Latham & Watkins report from Paris.

Founded in 2006 and headquartered in France, Spartoo SAS (Spartoo) is one of the leaders of the European online shoe retail market. On 31 May 2018, a week after the entry into application of the GDPR, France's Data Protection Authority (the CNIL) launched an on-site investigation of Spartoo in cooperation with other EU supervisory authorities. The CNIL eventually handed down its decision on 28 July 2020, imposing a €250,000 fine on Spartoo for the infringement of four different provisions of the GDPR. Spartoo had the right to appeal within two months of the decision. The case illustrates how the GDPR's "one-stop shop" mechanism can operate, and also provides insight to online retailers and other businesses on what to expect regarding GDPR enforcement in practice.

## The CNIL as Lead Authority

Under GDPR Article 56, the supervisory authority of the main or single establishment of a data controller is competent to act as lead supervisory authority for cross-border processing carried out by that controller.

Spartoo is incorporated in France and operates 16 retail websites for customers in 13 EU Member States[1] and the UK. The CNIL found that it was competent to act as the lead supervisory authority in regard to Spartoo's cross-border data processing activities. Consequently, the CNIL followed the cooperation mechanism provided in GDPR Article 60, meaning that the authorities in the Member States in which Spartoo operates had the opportunity to contribute to the CNIL's investigation and decision. In this case, the authorities of Italy, Portugal, and Lower Saxony (Germany) all presented reasoned objections to the CNIL's draft decision, which the CNIL took into account.

The proceedings carried out by the CNIL were concluded relatively quickly, given the number of authorities involved, and the final decision was adopted 26 months after the investigation opened. The deadlines provided by GDPR Article 60 are indeed quite short: the lead authority must submit a draft decision to the other authorities concerned "without delay"; the latter may express relevant and reasoned objections within four weeks; and their consultation of the revised draft must take place within two weeks.

## The CNIL's decision

The CNIL held that Spartoo was in violation of four different provisions of the GDPR:

1. Data minimization under Article 5.1(c).
2. Storage limitation under Article 5.1(e).
3. Right to be informed (transparency) under Article 13.
4. Security of processing under Article 32.

As a result, the CNIL imposed a €250,000 fine and ordered Spartoo to comply with the GDPR within three months of the decision, or face a penalty of an additional €250 fine per day.

Although Spartoo's financial statements are not publicly available, several press articles reported an annual global turnover of €250 million for the 2018 fiscal year. On this basis, the fine imposed by the CNIL would correspond to approximately 0.1% of Spartoo's annual global turnover, well below the 4% maximum limit set by GDPR Article 83.

The CNIL referred to a number of factors in its decision on the level of fine:

- The fact that most of the violations related to data protection principles that existed prior to the GDPR.
- The high-risk nature of some of the personal data (in particular bank details).
- The number and severity of the infringements (especially the systematic recording of employees' calls without a legitimate purpose or adequate information).
- The large number of data subjects impacted (several thousand).

The CNIL's order to remediate the breaches within three months was issued on the basis that it found Spartoo to still be in breach at the investigation's close (notwithstanding certain corrective measures already implemented).

## Data minimisation

Under GDPR Article 5.1(c), personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

The CNIL found that Spartoo's practice of collecting and storing all calls between its customers and employees for the purpose of employee evaluation and training was disproportionate and particularly invasive of employees' privacy. The CNIL also noted that while customers are given the opportunity to object to the recording at the beginning of each call, employees are not given the same option.

Furthermore, the CNIL noted the absence of technical measures to ensure that calls including customers' banking information were not recorded. The CNIL deemed the banking information to be unrelated to the stated purpose of the processing (i.e. employee training) and high risk given the potential harm to individual customers (i.e. accidental or unlawful disclosure of their banking information to third parties).

## Storage limitation

Under GDPR Article 5.1(e), personal data may only be "kept in a form which permits identification of data subjects for no longer than is necessary for the

purposes for which the personal data are processed."

The CNIL noted that Spartoo initially did not have a retention policy, and stored the personal data of its 25 million prospects indefinitely. Spartoo later adopted a retention period of five years from the date of last contact, which the CNIL found to be excessive.

During the investigation, Spartoo claimed to have implemented a new policy of contacting its former customers and clients for marketing purposes for up to two years after the date of their last activity. Although this retention period was deemed proportionate, the CNIL held that Spartoo was nonetheless in breach of the storage limitation principle by relying on the opening of a marketing email as customer "activity". The CNIL found this to be an insufficient indication of the interest of the data subject in the products and services, unlike, for example, clicking on a hyperlink included in a marketing email.

Furthermore, Spartoo's practice of retaining customers' and prospects' email addresses and passwords beyond the retention period was found to be non-compliant with the GDPR. The CNIL made clear in its decision that, at the expiry of the retention period, all personal data must be deleted and not simply made pseudonymous through, for example, a hash function.

### Transparency and the Right to Be Informed

Under GDPR Article 13, the data controller must provide data subjects with certain information, including the controller's identity, the purposes and legal bases of data processing, and the recipients or categories of recipients. The data controller must also specify whether personal data will be transferred outside of the European Union.

The CNIL found that Spartoo breached its obligations under this Article by failing to inform data subjects of the transfer of their personal data to Madagascar when calling customer service.

In addition, the CNIL held that consent should not be indicated as a blanket legal basis for all of the processing activities carried out by Spartoo pursuant to its privacy policy, as other legal bases, such as contractual necessity or legitimate interest, were also relied upon in practice and should therefore be specified in the company's privacy policy. The CNIL emphasized the need to identify and specify the legal basis for each specific data processing activity. Notably, the misidentification or failure to specify a legal basis did not appear to impact the CNIL's view on the lawfulness of the processing activities themselves, as long as a valid legal basis did in fact exist.

Finally, the CNIL found that Spartoo did not provide sufficient information to its employees regarding the existence and characteristics of the recording of their calls with customers, both with respect to data protection laws and applicable labour laws. The CNIL considered this lack of information particularly egregious as the practice lasted many years and could be regarded as a form of constant surveillance.

### Security obligations

According to GDPR Article 32, the controller or processor must implement security measures "to ensure a level of security appropriate to the risk".

The CNIL considered this lack of information particularly egregious as the practice lasted many years and could be regarded as a form of constant surveillance.

In assessing Spartoo's compliance with this Article, the CNIL noted that banking information is a type of personal data that can severely impact individuals in case of a security breach. In light of this, the CNIL found Spartoo's use of eight-character-long passwords, without any requirements regarding character types, to be insufficient, as such passwords are vulnerable to brute force attacks.

The CNIL referred to France's Information System Security Agency guidelines regarding passwords as well as its own recommendations from 2017 to justify this assessment. Specifically, the CNIL states that a password must be at least 12 characters long and include a minimum of four different types of characters if no other security measures are implemented at the log-in stage. If additional security measures are implemented, such as captcha[2] or account locking after multiple unsuccessful attempts, the CNIL considers a password of at least eight characters including at least three different types of characters to be secure enough.

According to the investigation, Spartoo requested that, for purposes of fraud prevention, customers send a scan of their credit or debit card by email, showing at least half of the card's numbers, the name of the holder, and the expiry date. The CNIL found that this practice encouraged customers to send, in an unencrypted form, the entirety rather than a truncated version of their bank card numbers. The CNIL considered such collection and storage of full customer card details to be in violation of Spartoo's security obligations, notwithstanding Spartoo's prior authorization from the CNIL to store bank card details in their truncated form.

### Practical implications

The CNIL decision sends a strong signal to online retailers and other businesses regarding the level of scrutiny that the CNIL and other supervisory authorities are likely to apply when investigating potential GDPR infringements. Whilst each supervisory authority has its own approach to enforcement, the CNIL decision was supported by a number of other supervisory authorities via the GDPR's cooperation mechanism, and gives a good indication of the standards expected by the supervisory authorities in practice. To minimize the risk of GDPR enforcement, online retailers and other businesses should:

1. Adopt a consistent high-watermark approach to GDPR compliance when engaging in cross-border data processing, as the designation of a lead authority does not shield entities from scrutiny by other

 

supervisory authorities, including those with potentially stricter approaches.
2. Consider prioritizing any compliance remediation efforts on long-standing data protection requirements that pre-date the GDPR, as supervisory authorities may be less tolerant of breaches in this context.
3. Ensure that each data processing activity has a clear and justified relationship with its underlying purpose, i.e. the nature and scope of the processing must be tailored to its purpose, not the other way around.
4. Define a sufficiently detailed and transparent data retention policy, and ensure the effective deletion of personal data at the end of the applicable retention period; supervisory authorities are taking an increasingly strict approach to long and unlimited retention periods of personal data (e.g., a high GDPR fine imposed by a German data protection authority was in relation to the unlimited retention of customer data).
5. Ensure that any local (or industry or technology specific) information security requirements, guidance, and best practices are properly integrated into the organization's systems and processes, to ensure adequate protection of personal data.
6. Be mindful that the obligations under the GDPR apply equally to internal as well as external data subjects; how an organization uses its employee personal data can be subject to just as much scrutiny as its use of customer personal data.

**AUTHORS**

Myria Saarinen is a Partner and Charlotte Guerin an Associate at Latham & Watkins, France.
Emails: myria.saarinen@lw.com
charlotte.guerin@lw.com

The authors wish to thank Alex Park in the Paris office for assistance in writing this article.

**REFERENCES**

1 These websites target customers in France, Spain, Germany, Italy, the Netherlands, Slovakia, Denmark, Poland, Sweden, Finland, Belgium, the Czech Republic, and Hungary.
2 A computer program or system intended to distinguish human from machine input.


ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

# Switzerland's DP Act revised

**David Rosenthal** of Vischer reports from Zurich on new aspects of the law which is expected to enter into force in 2022.

The splitting of hairs is now over and the revision of the Swiss Data Protection Act (DP Act) has finally been completed. Following the resolution of the last differences on "profiling", the Swiss Federal Parliament passed the new law on 25 September 2020. It is expected to come into force in 2022, with some sources even suggesting summer 2022. As a next step, the supporting ordinances will now be drawn up and submitted for public consultation. How fast things now progress will of course also depend on the EU: Switzerland is still waiting for the renewal of the European Commission's adequacy decision,

*Continued on p.3*

# Egypt's Data Protection Law enters into force in October

It is likely that the law will not be fully enforced until 2022, but businesses should start preparing now. By **Dino Wilkinson** and **Masha Ooijevaar** of Clyde & Co.

On 13 July 2020, Egypt's Government issued its long-awaited Data Protection Law[1] (Law No. 151 of 2020) (the Law), which establishes various standards and controls governing the processing and handling of personal data. The Law was published in the Official Gazette on 15 July 2020.

The Law is part of a growing trend of countries enacting comprehensive data protection laws, which

*Continued on p.6*



Issue 167 **OCTOBER 2020**

INTERNATIONAL report

ISSUE NO 167 OCTOBER 2020

**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@privacylaws.com

**CONTRIBUTORS**
**David Rosenthal**
Vischer, Switzerland
**Dino Wilkinson and Masha Ooijevaar**
Clyde & Co, United Arab Emirates
**Joan Antokol**
Park Legal, US
**Myria Saarinen and Charlotte Guerin**
Latham & Watkins, France
**Yen Vu, Trung Tran and Bao Nguyen**
Rouse, Vietnam
**Katharine Kemp and Graham Greenleaf**
UNSW, Australia
**Simon Frankel, Cortlin Lannin, Kathryn Cahoy and Rafael Reyneri**
Covington & Burling, US
**Yimika Ketiku**
Nouvelle Legal, Nigeria
**Oliver Butler**
University of Oxford, UK
**Camilla Tabarrini**
University of Venice, Italy

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
**Tel: +44 (0)20 8868 9200**
**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

## New laws adopted in Egypt and Switzerland

The influence of the EU GDPR continues to be felt far and wide. Egypt has adopted its first ever data protection law which enters into force on 16 October 2020 (p.1), and Switzerland has recently updated its 1992 data protection law, planning to retain its EU adequacy status (p.1).

The GDPR has also been a model for many African countries, several of which already have legislation in place. In this issue, we report on Nigeria's Data Protection Bill, 2020 (p.31).

How would a US federal privacy law interact with existing state level privacy laws (p.14)? In this issue we look at the private right of action under the California Consumer Privacy Act and how it might be expanded (p.29).

The *Schrems II* judgment of the Court of Justice of the European Union in July has had an impact on US business and is a major topic that will stay with us for some time, although the EU Commission is prioritising this work and is trying to find a solution for data transfers from the EU to the US (p.9). We may see revised Standard Contractual Clauses emerge before Christmas. An expensive alternative is using Binding Corporate Rules. Read on p.12 what the experience has been in 2020 with companies working with four national DPAs as lead authorities.

Professor Graham Greenleaf explores the relationship between trade agreements and new data privacy laws and Bills in Asia-Pacific countries (p.18), and together with Dr Katharine Kemp, the anti-competition developments in Australia regarding Facebook and Google (p.25).

We will return to these questions in our series of five *PL&B* webinars on German data protection legislative and judicial developments and their impact on business. The first webinar on 28 October will discuss how different laws are becoming more relevant to privacy issues, for example, in the Facebook decision of the Federal Cartel Authority (*PL&B International Report* December 2019 p.1) and the subsequent Higher Regional Court of Düsseldorf and Federal Supreme Court decisions. See www.privacylaws.com/germany for the programme and on how to register (p.8).

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

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 165+ countries alongside legal analysis, management guidance and corporate case studies.

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

**Stay informed of data protection legislative developments in 165+ 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 administrative 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 and reputation.**

## Included in your subscription:

**1. Six issues published annually**

**2. Online search by keyword**
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.

**3. Electronic Version**
We will email you the PDF edition which you can also access via the *PL&B* website.

**4. Paper version also available**
Postal charges apply outside the UK.

**5. News Updates**
Additional email updates keep you regularly informed of the latest developments in Data Protection and related laws.

**6. Back Issues**
Access all *PL&B International Report* back issues.

**7. Events Documentation**
Access events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

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

**privacylaws.com/reports**

"I've always found *PL&B* to be a great resource for updates on privacy law issues, particularly those with a pan-EU focus. They are almost always the first to an important privacy law story, meaning that I (and all of my team and most of my clients) will quickly open a mailshot from *PL&B* to see what's going on in the world of data protection."

**Matthew Holman, Principal, EMW Law LLP**

## UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of data protection legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business strategy.

## Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

## Satisfaction Guarantee

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