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.

Switzerland... from p.1

which allows unhindered data transfers to Switzerland. The EU could put pressure on Switzerland to speed up the process of the revised law entering into force.

Change for personal data of legal entities

Although the 1992 DP Act has been totally revised, the private sector will in general not have to change the way it processes personal data. The basic principles of data processing remain unchanged in the new DP Act. Although certain general protections continue to apply, there is one exception: personal data of legal entities are no longer protected. The Swiss concept remains unchanged in that data processing in the private sector is in principle permissible and a justification (or "legal grounds") is required only in certain situations.

Thus, the DP Act continues to deviate from the EU General Data Protection Regulation (GDPR) under which the processing of personal data is generally prohibited unless there is a legal ground such as consent, the performance of a contract, a sufficient legitimate interest or a legal provision in law.

Consents: Less restrictive than under the GDPR

Switzerland also does not go as far as the GDPR in terms of the requirements for valid consent. Essentially nothing changes here compared to the current legal situation in Switzerland, with the exception of a minor change with respect to profiling (see below). There is no need to inform individuals about the possibility of withdrawal of consent, and multiple consent declarations can be combined.

The grounds on which data processing activities can be justified remain more or less the same as in the current DP Act, and go beyond what is provided for in the GDPR. What has been worded slightly more restrictively is the justification for non-personal processing purposes (for example, statistical uses) and the justification upon which credit agencies have been relying. They now have to delete data that is older than ten years in the event that a data subject so requests.

WHAT WILL CHANGE IN 2022?

- New information and documentation requirements similar to the GDPR → create and update documentation
- New risk of fines with regard to data exports and processor agreements → verify and amend contracts
- Notification obligation in the case of data breaches similar to the GDPR → introduce a process as under the GDPR
- The new Data Protection Act (mostly) does not go beyond the GDPR, but is not identical → check for differences

The principle of "Privacy by Design" is now also explicitly included in the law, but strictly speaking it has always existed – even under the current DP Act. Indeed, the only provision that is new is the Swiss version of "Privacy by Default", which is relevant only in cases where a provider of an (online) service provides data protection settings as part of such service, which must be set by default so as to limit data processing to the intended minimum.

More governance: Inventory, DPIA, reporting

Much like in the case of the GDPR, the main changes in the new DP Act are:

- new governance obligations, such as the requirement to maintain records of data processing activities,
- the obligation to report data losses and other data security breaches to the Federal Data Protection and Information Commissioner (FDPIC), and
- the obligation to carry out data protection impact assessments (DPIA) for sensitive data processing.

All three requirements are comparable to the corresponding provisions under the GDPR, and will result in additional workload for companies that have not already undergone the process for the purposes of the GDPR. Those who have done so can adopt the existing data processing inventories more or less directly and have their data breach notification procedures amended to also comply with Swiss law. The DP Act provides for slightly different thresholds as to when a notification becomes necessary, but essentially works along the same lines as the notification obligation under the GDPR.

Swiss lawmakers have also "copied" the concept of a DPIA, which so far has not formally existed under Swiss law although it is already well known under Swiss data protection law as "good practice" in the case of sensitive data processing activity. While it does involve some work, it is not particularly difficult to create a DPIA. It essentially consists of a description of a planned data processing activity, assessing the negative consequences for those affected and detailing the countermeasures taken as a result to mitigate those consequences.

No duty to appoint a data protection officer

Whereas the new DP Act provides that companies can appoint what is referred to as a "data protection advisor" (which, in essence, is a data protection officer), there is – unlike under the GDPR – no obligation to do so. Yet, most mid-sized and larger companies will not be able to implement data protection properly unless they have appointed a responsible person to deal with data protection. Furthermore, foreign companies with significant activities in Switzerland will have to appoint a Swiss representative, but we expect only a few companies will be subject to this requirement. Thus, the obligation is not as stringent as the corresponding provision in article 27 of the GDPR.

Right to information is restricted

The rights of the data subjects are somewhat extended, but at the same time also defined slightly more clearly. While it will be easier for data subjects to request their own data from a company, the new DP Act also offers new arguments for rejecting abusive access requests. For example, only personal data "as such" may be requested and only what it is necessary to assert data protection rights. The "right to be forgotten" known from the GDPR existed under the DP Act all along and will remain. It is still not absolute, but provides for a balancing of interests. Likewise, the principle that data may only be processed as far and as long as necessary continues to apply.

Entirely new to the DP Act, however, is the right to data portability, which Swiss lawmakers copied from the GDPR. It actually does not have

much to do with data protection, but enables consumers to obtain their data stored with online or other services providers in order to transfer such data to competitors.

Also completely new is the right to demand that a person reconsiders important decisions that were made exclusively on an automated basis and which by their nature allow for interpretation. The provision is comparable to the GDPR provision on automated individual decisions, but the DP Act only requires a controller to inform individuals about such decisions and allow the data subject to request human intervention.

Data processing: Checking contracts

The requirements for contracts with data processors, i.e. companies to whom controllers delegate their own processing of personal data, such as cloud service providers, have been tightened up somewhat in that the use of subcontractors must now be approved by the controller. Yet, the new provisions still fall short of those of the GDPR. Since the requirements under article 28 GDPR are nowadays considered standard in the industry, we do not expect any problems for controllers to ensure compliance with the new rules under the DP Act. The clauses agreed with processors will usually only have to be adapted to refer not only to the GDPR but also to the DP Act.

Privacy policy becomes mandatory

The obligation to provide information has been expanded under the new DP Act. This means that companies must have a data protection declaration in which they provide certain mandatory information regarding the personal data they collect. This type of information is usually provided on the companies' websites and by means of links included in their forms and contract terms and conditions. Conceptually, the information obligation under the new DP Act is very similar to the information obligation under the GDPR, but does not require as much mandatory content as the GDPR.

The only exception is the obligation of a controller to indicate the countries to which personal data is exported and the legal provisions on which the company relies in doing so. However, in our view, it is not necessary to list each and every country, as terms such as "Europe" or "worldwide" should work, too. If a company has appointed a data protection advisor or a representative, information on this subject must also be provided. As a consequence, certain adjustments to the existing data protection statements are therefore necessary, but we do not expect this to create any big issues.

Transfers abroad easier

The revised DP Act governs cross-border transfers of personal data slightly differently than in the past, but the practical consequences are very limited. It is now up to the Federal Council to determine the countries that are considered to have an adequate level of data protection and to which data can be exported without special precautions. Until now, it has been the DPA (FDPIC) who maintained a list of countries with the FDPIC's President's assessment on the topic. But this list was not binding and this is also the reason why the effects of the Court of Justice of the European Union's decision "Schrems II" in Switzerland were much more limited than in the EEA.

The EU Standard Contractual Clauses for data exports can still be used but the obligation to notify them to the FDPIC has been removed from the new DP Act. The disclosure of personal data to foreign authorities will also become easier; previously this was often only possible in the context of judicial proceedings.

More fines possible

The enforcement of the DP Act will also change under the new law. In the past, the FDPIC was only able to issue "recommendations" to data controllers and processors who in his opinion did not comply with the DP Act. If they did not comply with his recommendation, he could sue them. In the future, he will directly issue orders against controllers and processors. For example, he will be able to order that a particular data processing activity be stopped. That said, these new powers will also result in the FDPIC's procedures becoming more complicated and requiring more resources than those under the current DP Act. It remains to be seen whether the new concept will lead to more enforcement, or result in actually fewer cases given the FDPIC's constant understaffing. The FDPIC will still be unable to impose fines.

The right to impose fines lies with the Cantonal law enforcement authorities (which are not specialized in data protection), and the catalogue of fines been significantly expanded. In the past, fines were possible for the violation of the duty to inform individuals, the duty to comply with the data subject access right and the duty to cooperate with the FDPIC. Now, violations of:

- the provisions on data exports,
- the provisions on commissioning processors, and
- certain violations of data security measures can also be fined.

The fines are primarily to be paid by the decision-makers but only if they acted intentionally. They can be found liable up to the amount of 250,000 Swiss francs (€230,000). Although these amounts pale in comparison with the amounts under the GDPR, they will likely be even more effective given that they are of a personal nature and cannot be insured. We assume that fines for data protection violations will continue to be the exception in Switzerland. Furthermore, violations of the fundamental principles of the DP Act continue to be exempt from punishment – an important difference to the GDPR. In addition, the revised DP Act introduces a general professional secrecy for all professions (with fines of up to 250,000 Swiss francs and a new provision against identity theft.)

No consent necessary for profiling

The main bone of contention in the deliberations on the new DP Act was "profiling", which has the same meaning under the DP Act as under the GDPR. Noteworthy, as under the GDPR, the legal significance of "profiling" as such is very limited. Profiling is, in essence, the automated formation of opinion on certain aspects of an individual. Although profiling is a defined term in the new DP Act, there are hardly any provisions of the DP Act that refer to it, at least with regard to the private sector. Unlike what has gen-

erally been reported, the new DP Act does not provide that profiling requires consent. What the new DP Act does say is that if consent is required in a particular case, such consent has to be of an express nature in the case of profiling with a "high risk". Profiling is considered high risk if it results in a more detailed profile of an individual. This is already in line with the current legal situation under the existing DP Act. In other words almost nothing actually changes under the new DP Act. Although profiling as such does not require consent, it is, of course, already possible that a data processing operation goes so far that justification is required. Consent is one possible form of justification, but the controller may also be able to rely on an overriding private interest depending on the circumstances.

Need for action

What needs to be done now? Most companies should have enough time to implement the most important provisions of the revised DP Act. First, they should review their data protection statements in light of the new requirements and adapt them or, if necessary, create new ones if they have none in place. The most time-consuming part of the process is usually the internal review of data protection activities to ensure that all cases in which the company procures personal data are covered. Once a company has obtained this information, it can create or update the data protection statement and establish an inventory of data processing activities. If such statements and inventories have already been created for the purposes of the GDPR, they can to a large extent be re-used for the DP Act.

In a further step, controller-processor relationships need to be identified and related contracts checked and adapted as per the new, stricter rules of engagement. If this work has already been done for the GDPR, again, not many changes will be necessary. What is usually necessary is to expand the references to the GDPR to also include the DP Act. In a similar manner, controllers and processors should identify international data transfers and verify whether they fulfil the DP Act's requirements, given that non-compliance can be fined going forward. If the DP Act's current requirements are fulfilled, most likely no changes are necessary.

Companies should also implement a process for data protection impact assessments and, if necessary, appoint a data protection officer, even if not required by law. A process for identifying, analysing, reporting and handling data security breaches (which term includes unintentional data losses and misdirected emails) should also be introduced. Every company should also have a process – if not already in place – for responding to requests from affected individuals e.g., those requesting access to their personal data. When referring to "processes", we mean that a company should at least appoint an individual to be responsible for handling the relevant topic who knows what to do in each case or where to get the relevant information on what should be done.

Finally, automated individual decisions should be identified and, if relevant, data subjects should be informed and given the opportunity to ask for human intervention. Furthermore, processing of genetic and biometric data as well as data for non-personal purposes and creditworthiness should be identified, checked and adapted to the new requirements. Of course, existing training should also be adapted to correspond with the requirements under the revised DP Act and it may make sense to verify implementation of the new requirements by way of conducting audits.

Those who have already implemented the GDPR requirements in their organizations will not have to make much additional effort. The main relevant amendments in the new DP Act with practical significance are regarding:

- the obligation to provide information which requires information on relevant countries and legal bases in the case of data exports,
- the rights of data subjects, in particular, the new DP Act provides for different exceptions,
- the obligation to report data breaches - there is no 72-hour obligation and the thresholds are slightly different, and
- the appointment of a data protection officer or representative – most companies will not formally require a data protection officer or representative.

AUTHOR

David Rosenthal is a Partner at Vischer in Zurich, Switzerland.
Email: drosenthal@vischer.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.