# Use of AI/Machine Learning to boost regulatory workflow and efficiency

**Peter McLaughlin** and **Ashfin Islam**, Armstrong Teasdale LLP explain the opportunities with Artificial Intelligence and Machine Learning for Supervisory Technology, SupTech.

Data protection regulators are facing a big data problem. Amid rapid innovation and steadily increasing rules across the regulated entity landscape, the fast-growing number of firms, disclosures and complaints they must manage is straining limited resources. SupTech, short for supervisory technology, is the application of emerging technologies to improve how a regulating or supervising agency in any sector – financial, export control, or data protection – conducts its regulatory duties. (Of course, the opposite side of SupTech is RegTech, which is focused on the use of tech to support an organization's compliance efforts.) There are varying but similar definitions of SupTech. According to a World Bank Group report, SupTech "refers to the use of technology to facilitate and enhance supervisory processes from the perspective of supervisory authorities." The Bank for International Settlements (BIS) defines SupTech as "the use of technology for regulatory, supervisory and oversight purposes."

## How to enhance efficiency with SupTech

SupTech is focused on maximizing efficiency by applying automation, optimizing operational and administrative operations, and digitizing the working tools and data. SupTech can be at its most robust when incorporating variants of artificial intelligence (AI) and machine learning (ML). At its most transformative, SupTech can unlock the potential of mountains of data, robust communication workflows and deep regulatory knowledge. It can even serve as a springboard to more comprehensive risk oversight and better, more effective application of regulations. SupTech is not limited, however, to the general enhancement of the overall capacity and efficiency of supervisory oversight. Its applications may potentially assist in more efficient detection of misconduct. Further, SupTech may be able to better determine compliance with and enforce regulatory requirements that are principle-based or comprise judgment-based rules, such as assessing a data controller's policies and procedures against the EU GDPR and guidance. These solutions can further reduce costs related to regulatory reporting, data collection, and risk management.

What is the leadership of a DPA to do with all of this? It is impossible to simply put aside the challenges of resources, but the status quo is untenable. Likewise, building a proprietary system that reflects the DPA's identified needs is nearly impossible – technology budgets simply aren't large enough. That means the most logical way forward is usually to work with a third-party SupTech provider with the necessary skills and experience. This presents unique opportunities and challenges for regulators, especially in the AI/ML space. Regulators will evaluate potential SupTech providers based on several important technological factors, including flexible, scalable technology; collaboration and communication; expert content; and their ability to manage people and change.

First, the ideal SupTech is flexible and scalable. Solutions should be able to integrate and communicate with just about any other system or content in the supervisory workflow. The benefit of using AI/ML is to collect and analyze huge troves of data. One of the benefits of cloud infrastructure is enhancing computational performance so that DPA staff spend less time worrying about server capabilities and more time on core supervisory functions. However, some supervisory institutions, such as central banks, have reportedly been slow to adopt completely cloud-based infrastructures. One solution is a hybrid model where the cloud infrastructure works together with on-premises technology. The ability of a SupTech provider to be flexible and scalable with the needs of a DPA is key to fostering adoption.

To further encourage acceptance, SupTech should be able to collaborate and communicate with all varieties of systems or content in the supervisory workflow. SupTech must facilitate smooth communication and collaboration between the regulator and the regulated entity as well as individuals who make requests and/or complaints at every step of the process. For example, ChatGPT and advanced large learning models (LLMs) empower chatbots to interact with data controllers and individual data subjects more efficiently. Similarly, natural language processing technologies (another AI/ML flavour) can more efficiently absorb and audit documentation produced by an organization under review. These impressive tools and technologies are less helpful if the SupTech cannot talk directly and efficiently to the systems it seeks to supervise.

## EU supports SupTech initiatives

In 2020, the Commission stated that by 2024, the EU aims to put in place the infrastructure allowing the widespread use of SupTech tools. While focused on regulation of digital finance, the Commission, together with the European Supervisory Authorities are attempting to create an infrastructure of supervisory data to help ensure that:

"1. supervisory reporting requirements (including definitions, formats, and processes) are unambiguous, aligned, harmonised and suitable for automated reporting,
2. full use is made of available international standards and identifiers including the Legal Entity Identifier, and
3. supervisory data is reported in machine-readable electronic formats and is easy to combine and process. This will facilitate the use

of RegTech tools for reporting and SupTech tools for data analysis by authorities."

In October 2022, the European Commission sought to further clarify procedural aspects regarding the enforcement of the GDPR in the Commission's 2023 Work Programme. This follows the European Data Protection Board's statement and subsequent letter on enforcement cooperation enumerating a list of procedural aspects to harmonize GDPR enforcement at the EU level. The attempt to harmonize and empower individual supervisory authorities comes at a great time in the evolution of SupTech. Specifically, the European Commission found that certain entities with operations in multiple jurisdictions were poorly suited to implement the same reporting solution for all their locations due to cross-border supervisory expectations and technological capacity.

Collaboration among DPAs, regulated entities, and technology service providers within and across jurisdictions is a key consideration for developing beneficial SupTech solutions. Ideally, this infrastructure will promote the sharing of data between supervisory authorities. By thoughtfully and precisely working with SupTech providers and regulated entities, DPAs can create templates and other procedural tools within SupTech solutions to foster procedural cooperation, and ultimately adoption.

## DPAs could benefit from using prebuilt templates

Any DPA-specific SupTech system should offer prebuilt templates. This will mean configurable forms for the EU General Data Protection Regulation (GDPR) and relevant national and state laws out-of-the-box. Further, an effective system will also have a strong ability to implement specific content and rules supplied by each adopting regulator. For example, the Irish , the Japanese, and the Australian DPAs individually have their own supervisory processes and experiences, not to mention pain points. The incorporation, or rather, the translation of regulatory content into machine-readable regulations may enable a computer system to process those rules against DPAs' policies and procedures.

The effectiveness of SupTech solutions is currently limited by both poor data quality and ineffective use of supervisory tools. Compounding this concern is IBM's reporting that poor data quality represents a $3.1 trillion dollar loss in the US economy alone. SupTech solutions that place an emphasis on global and local expertise are able to more readily adapt their technologies to the required regulatory landscape. As discussed below, there is significant risk of incorporating human bias in algorithmic decision making, which is highlighted by the black box nature of many SupTech solutions. The risks[1] are intensified when DPAs lack the necessary expertise or skills to deal with these obstacles. More emphasis placed on expert content will lead to better data quality and allow AI/ML capabilities to more accurately analyze data with respect to the regulatory scheme.

Despite SupTech's rapid evolution, the human element of a DPA's activities remains an important fulcrum. The complexity of rules and their interpretation is a part of this, but also the difficulty of managing change within any organization (even a government body) cannot be underemphasized. All of this cutting-edge technology must benefit the individual regulators and be managed as an assisting tool rather than a looming threat. And, any change to tools and systems requires some level of change in how people do their jobs. Therefore, the best SupTech will be developed with people in mind. While SupTech can assist with the supervisory functions, it is still people who are ultimately responsible for interpreting the AI/ML analysis into actionable enforcement. Ideally SupTech will keep in mind the human element, understanding that SupTech by itself is not the final end point of data protection supervision.

## The obstacles involved with using SupTech

While there are seemingly endless benefits of SupTech, all integrated AI/ML systems face similar and daunting issues. First, the increasing variety of interconnected systems that make SupTech so enticing presents myriad issues. For example, DPAs must be wary of the way distributed ledgers often employed by SupTech solutions can compromise compliance with data protection regulations, which would be ironic. While the distributed ledger technology offers transparency and immutability, there are many global data privacy regulations that require anonymization and deletion of personal data that would be hamstrung by these solutions. Additionally, as systems and platforms become more connected, the scope of potential cyberattacks grows. There are more entry points for cyberattacks and more voluminous data for potential bad actors to target.

This additionally leads to operational risk. Discrepancies in regulated organizations' network infrastructure, whether it be non-conforming policies and procedures or data breaches, can have negative cascading effects on a supervisor's activities. A breach in one of these interconnected systems can cripple entire regulatory ecosystems.

Next, a looming issue in the AI/ML revolution is that programming and algorithms are still developed by humans with inherent bias and ignorance. The conclusions reached by algorithm-driven SupTech are invariably colored by this risk. Massive amounts of data are processed, and the technology spits out a result. It is difficult for most people to understand the algorithm's logic or decision-making process.

This black-box issue creates further legal issues. Any regulated organization should be able to request a full, comprehensible accounting of the decision-making process. If the SupTech's engine is proprietary, it might become very difficult to audit these automated decisions. As a result, human intervention must be at the forefront for DPAs utilizing SupTech. People, not an algorithm, must be able to identify any idiosyncrasies and validate that the algorithm's results were equitable and accurate. Skilled human oversight is an absolute must. While the SupTech solutions can provide suggestions and recommendations, the final decisions on enforcement actions are ultimately a human judgement and responsibility.

Next, SupTech must take into account the number of legacy processes used by DPAs and data controllers

such that these processes can be linked to the SupTech solutions and ensure that there is no data loss. Otherwise, the SupTech's decision-making process is compromised by an incomplete or an inaccurate data set.

Finally, DPAs are restricted by financial and human resources. Budget restraints and governmental procurement rules may hinder the development and use of SupTech. The cost of the software, user licenses, any hardware upgrades, and the people-hours needed to implement and scale a revolutionary system are significant barriers for already constrained DPAs. One example is that supervisory authorities may be prohibited from processing supervisory functions in the cloud, requiring local server solutions that may be more expensive and time-consuming. DPAs must navigate these budget restrictions to efficiently design their use of SupTech.

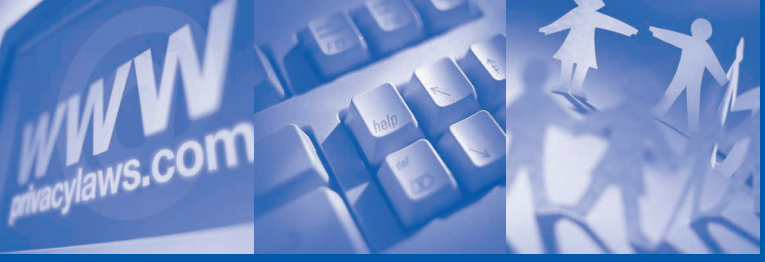
Opportunities abound for both DPAs and the prospective technology suppliers, but the path to these greater efficiencies has its distinct resource demands.

**AUTHORS**

Peter McLaughlin is a data privacy partner and Ashfin Islam is a data privacy associate at Armstrong Teasdale LLP, Boston, US.
Emails: PMcLaughlin@Atllp.com
Aislam@Atllp.com

**REFERENCE**

1 See www.oecd-ilibrary.org/sites/d478df4c-en/index.html?itemId=/content/component/d478df4c-en#section-d1e12945




ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

# How consistently is the EU GDPR being enforced?

The European Union's data rules have built-in consistency mechanisms. After five years of operation, how well are they working and what does the future hold? **Tom Cooper** reports.

The uniform application of the EU's General Data Protection Regulation (GDPR) across the bloc's 27 Member States, each with a different history, legal system and attitude to data protection, was always going to be a challenge. Nevertheless, that is the European Data Protection Board's (EDPB's) remit under EU law.

In May, the board elected Finland's Data Protection Commissioner, *Anu Talus*, as its new chair[1].

*Continued on p.3*

# Texas enacts comprehensive privacy law

**Jorge Ortiz**, **Nicholas Shepherd**, and **Lindsey Tonsager** of Covington & Burling analyse the law which enters into force in July 2024.

On 18 June 2023, the Governor of Texas signed into law the Texas Data Privacy and Security Act (TDPSA), making it the 12th state overall in the United States, and seventh in 2023 alone, to enact a comprehensive privacy law.[1]

With approximately 30 million inhabitants, Texas is the second-most populous state (behind only California) to pass a privacy law of this scope and magnitude. The TDPSA

*Continued on p.4*



Issue 184 **AUGUST 2023**

INTERNATIONAL report

ISSUE NO 184 AUGUST 2023

**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**
**Jorge Ortiz, Nicholas Shepherd, and Lindsey Tonsager**
Covington & Burling LLP, US
**Pablo Palazzi,**
Allende & Brea, Argentina
**Peter McLaughlin and Ashfin Islam**
Armstrong Teasdale LLP, US
**Nana Botchorichvili**
IDEA Avocats, France
**Juliette Faivre**
University of Cambridge, UK
**Asher Dresner**
Freelance writer, UK
**Tobias Lunn**
University of Nottingham, UK
**Gabrielle Hornshaw**
University of Nottingham, UK

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

# Future prospects for the EU-US privacy framework

Organisations have been pleased to see the adoption of the new EU-US Privacy Framework in July (p.7). It is almost certain that a legal challenge will arise – nevertheless companies now have some breathing space provided that companies sign up to the pact enthusiastically and implement their commitments in the US.

The next step is the EU Commission's long-awaited review of the existing adequacy decisions. Argentina, which is one of the beneficiaries, is now modernising its law to meet the higher GDPR-level of adequacy (p.17). The bill is based on the EU GDPR and the Council of Europe Convention 108+.

On the back of the EU-US decision, we can expect a UK decision soon, as well as Switzerland taking similar measures. But what about adequacy at US state level? The trend of adopting state level consumer privacy laws continues with Texas (p.1) and Oregon (p.6). There have already been speculations about California being a likely candidate for adequacy as it has a stronger law than the other states. Also possible are sectoral arrangements which would benefit the areas currently not covered by the Privacy Framework, such as financial services.

The Cambridge Analytica saga continues, as witnessed by our expert panel at *PL&B's* summer conference (p.14). In Australia, the Privacy Commissioner and Meta have now been ordered by the federal court to engage in mediation. This is to end the costly legal proceedings over the scandal which started five years ago.

Some worrying developments can been seen in the adoption of generative AI (p.28). The EU is not just paying attention but is at the forefront with its AI Act, and evaluating the impact of AI in the metaverse from many viewpoints (p.6). On the positive side, SupTech which includes AI elements can help DPAs with their workload (p.18).

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 180+ 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 180+ 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 in online format 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

"*PL&B UK and International Reports* are valuable and trusted resources for our office, offering timely, in-depth analyses about emerging issues in the world of global data protection. This publication is *de rigueur* for anyone who works in the fast-paced and constantly evolving privacy field."

**Michael McEvoy, Information and Privacy Commissioner for British Columbia, Canada**

## UK Report

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

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

## 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.