

A CPO Wishlist for EU Privacy Reform

Jay Cline

(IAPP, [IAPP - International Association of Privacy Professionals - A CPO Wishlist for EU Privacy Reform](#))

Chief privacy officers may get their wish after all. The European Commission this past June started the process to review EU data protection law. Taking this cue, one of Europe's more outspoken data protection commissioners called for a complete overhaul of the EU Directive on Data Protection (95/46/EC).

"European data-protection law is increasingly seen as out of date, bureaucratic, and excessively prescriptive," said UK Information Commissioner Richard Thomas to a July privacy conference in Cambridge.

To be sure, the Directive can be credited with many positive accomplishments, including the adoption of privacy laws by most industrialized countries and the elevation of privacy as a priority in many corporations. But what parts of the Directive could use a tune-up? We posed this question to privacy officers and advisers in Europe, the Americas, and the Asia-Pacific region. Their responses form a list of five main wishes.

1. Radically change the requirement for data-transfer documentation.

The overwhelming sentiment expressed by respondents from all regions was to abolish or fundamentally change Articles 25 and 26 of the Directive. These provisions famously prohibits transfers of personal data outside of the European Economic Area to "inadequate" destinations unless certain conditions are met, such as the documentation of model contracts or binding-corporate rules. The prevailing practice of the Article 29 working party—the EU's implementing arm for the Directive—to define an "adequate" destination for EU data to be a country with national legislation similar to the Directive has emerged as a principal flashpoint.

"Adequacy"

"The EU approach based on 'adequacy' hasn't worked," remarked Malcolm Crompton, former privacy commissioner of Australia and now head of Sydney-based Information Integrity Solutions. Crompton, who was instrumental in shaping APEC's outcome-based approach to transborder dataflows, cites the small number of countries deemed adequate by the EU as evidence of its ineffectiveness.

The global privacy strategy and policy manager for a large technology company echoed this sentiment: "In the electronic age, data crosses borders constantly and repeatedly, and something more flexible than 'adequacy' status or tons of model contracts needs to be in place to accommodate this."

"The directive, by focusing on adequacy for data transfers, is culture-centric," replied Martin Abrams, executive director of the Centre for Information Policy Leadership at the law firm Hunton & Williams.

"There are three aspects to privacy: security, prevention of the harmful application of information, and the cultural aspects of privacy," he added. "The new Directive may demand

respect for these cultural aspects of privacy, but not adoption by others who don't share these values."

The privacy attorney for a U.S.-based hotel company stated that the EU criterion for adequacy shouldn't be whether a country has sufficient national privacy legislation, but "whether or not the company [making the data transfer] has implemented sufficient controls around the personal data it processes."

"If I could change one thing about the Directive," opined Peggy Eisenhower, head of U.S.-based law firm Privacy and Information Management Services, "I would add an additional derogation to Article 26 so that Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:
(f) the data controller has taken reasonable measures to ensure that an adequate level of protection will be provided for the data at all times."

"The privacy protections would still exist, but without the administrative burdens of model contracts or the costs of trying to get a BCR (binding corporate rule) approved in each and every country," she added.

Eduardo Ustaran, head of the privacy practice at London-based law firm Field Fisher Waterhouse, suggested a similar solution.

"European law could continue to afford the same protection by simply making EU organizations responsible for all personal information in their possession, including information that has been transferred to a third party outside Europe, and by imposing a requirement to employ contractual mechanisms, corporate codes of conduct, or other means to provide a comparable level of protection while the information is being used by a third party."

The CPO for an information-services company concurred: "More and more data is moving around the world. These data flows greatly benefit the consumer wherever they live. Obligations to notify the consumer if data is moving outside Europe should not be required if the data controller takes full responsibility for protecting the data and making sure all appropriate use restrictions are honored."

Registration of databases and data transfers

Several respondents also found fault with the related requirement by several EU member states to register with them corporate databases and external data transfers.

"The notification system is not adding value and is not an appropriate system in a global economy," the German-based CPO of a technology company reported. "I happen to agree with the British information commissioner."

"I think it's important that any modifications to the Directive take into account the near-continuous global flow of data that occurs today," said Oracle's Chief Counsel of Privacy and Security, Peter Lefkowitz, "as opposed to the point-to-point transfers that were prevalent when the Directive was being considered."

"A number of the Directive's practical requirements," he added, "are vestigial remnants of a

different technological era, and they arguably do more to restrict commerce with the EU than to ensure that data is protected appropriately."

The CPO of a global hotel company also hopes to see a move away from regulating individual data transfers. "In today's connected world, it is difficult and challenging to assess, enforce, or tightly control transfers of data across national borders," the CPO said.

The privacy leader for a financial-services company hopes to see the elimination of the requirement for data-protection authorities to approve EU data exports.

"The rest of the world understands that this bureaucracy does little to help enhance privacy, and all it does is add cost and complexity to data transfers," he said.

A privacy attorney for a global manufacturer stated that "the processes for notifications to the various DPAs (data-protection authorities) should be made consistent or scrapped entirely."

"Notifying the DPAs of how a multinational company processes personal data is extremely burdensome, time-consuming, and costly," he added. "It also fails to drive the company to any greater degree of compliance."

Alternative solutions

Several respondents offered ideas for improving the way Europe meets its objectives relating to the registration of databases and data transfers.

Jose Luis Badia, commercial counselor for DuPont, said "I definitely would like to see a change in the way of doing international data transfers in a more homogeneous manner, by having a one-stop shop at the European level, setting up the standards without having to go through all the different DPAs."

"The current system is unpredictable and very expensive," he added.

Becky Burr, a partner with law firm WilmerHale, also hopes for a more centralized approach. "The current process is expensive and complicated. Even companies that comply with the principles, and try to comply with the notification requirements for processing and transfer, are inevitably out of compliance with the formalities."

Claus-Dieter Ulmer, data protection officer of Deutsche Telekom, would like to see the Directive treat affiliated legal entities as a single unit rather than as third parties requiring consent for data transfer. "[Affiliate arrangements] normally have no impact on the internal processes and procedures for the handling of personal information," he explained. "So what we need is a "Corporate Group Clause" that defines corporate groups—under certain preconditions—as a subset of a legal entity."

The Data Protection Officer of another large German corporation concurred: "Internal shared-services architectures are hampered severely by legal requirements which treat data flows to a subsidiary of the same group in the same way as if these data would be given to external third parties."

The CPO of one of the largest financial companies in the world applauded the EU's adoption of

binding-corporate rules as a way of simplifying DPA notification requirements. He suggested that the Article 29 Working Party extend the BCR concept so that four different types of interrelated companies could apply under the same BCR umbrella: "participants located within the EU; participants in the EU and affiliates in other countries; participants in the EU and third-party service providers in other countries; and participants in the EU and countries that have adopted adequate arrangements under the APEC or other privacy requirements."

Judith Beach, CPO of Quintiles, offered a similar solution. "It would be a breakthrough to see Binding Corporate Rules for particular industries," she said. "The EU could have a big impact, for example, if it approved a standard BCR for the pharmaceutical industry. Pharma companies could adopt this BCR and be automatically approved by the EU member states."

2. Harmonize EU member state implementation of the Directive.

The rejection of the EU Constitution by France, the Netherlands, and Ireland portends a long and uncertain path ahead for European political unity. The privacy leaders we contacted see this retreat from a "United States of Europe" already affecting their work.

According to the privacy attorney for a global communications company, his main concern is "the lack of consistency in interpretation and implementation of the Data Protection Directive across Europe."

"The Directive was partially intended to have a harmonizing effect vis-à-vis member-state law," explained. "However, differences in interpretation by European policymakers are still somewhat widespread. Examples include differences in notification requirements, data-security standards, data-retention limits, transborder dataflows, and employee monitoring."

"It would be beneficial to data controllers and data subjects alike if there was a more concerted effort, whether it be via the Article 29 Working Party, the Commission, or the Data Protection Supervisor, to issue more consistent guidance on rights and responsibilities under the Data Protection Directive and related omnibus measures."

The CPO of a global consumer-goods company agreed, stating that working with "27 different regulatory requirements adds months to any initiative we want to roll out globally."

The privacy counsel for a business-services company expressed the same sentiment. "The one change that we'd like to see in the EU directive is: consistency across the Union. As is currently the case across the 27 EU countries, the local privacy laws and their implementation vary widely. In our case, it ranges from us not being permitted to file anything with the local DPA since we are not a registered organization in that jurisdiction, to a simple Web filing, to a long formal filing and review process prior to having a data processing permit granted."

The privacy attorney of a large, U.S.-based retailer also hopes for a higher degree of coordination between member states on international data transfer issues. "We need something more robust than Safe Harbor, and simpler than today's Binding Corporate Rules," he said.

The privacy counsel for a technology corporation stated that "I would prefer that they not open up the 95/46 Directive."

"Most of the issues I have are with the implementation by individual member states," he explained, "and the lack of predictable and harmonized guidance in enough areas."

3. Better define standards and terms within the Directive.

Commissioner Thomas criticized the Directive for being "excessively prescriptive," but several privacy leaders we contacted hope that any review of the Directive will result in more precise definitions in several areas.

"I think the Directive is vague and offers much to interpretation," stated the privacy director for a consumer-services company. "We spend a lot of time responding to customers who think they understand the Directive enough to point out where we are in violation of the rules. We look to counsel for guidance who then interprets the Directive a bit differently."

Eisenhauer hopes the EU will add specificity to the concept of "personal data" whereby "data is only subject to the directive if used in an identifiable manner." As examples, she points to IP addresses and data collected for medical research that, while containing identifiable characteristics, are often not used in ways that could identify individuals.

David Hoffman, director of security policy and global privacy officer for Intel, stated that "the one thing I would focus on would be an analysis of whether the Controller/Processor distinction is a useful construct in today's data processing world."

Ustaran argues that a change of focus is needed: "The responsibility for legal compliance should follow the ambit of data uses, not the [Controller/Processor] label attached to those using the information."

The privacy counsel for a large dot-com concurred: "I would change the focus of data protection regulation from what I would call a "transfer-centric" model to a "use-centric" model."

"That is, change the focus of the law to the intended use of the data," he continued, "rather than what entities have access to the data."

Ustaran also hopes the Commission will bring more clarity to the definition of "sensitive personal data" within the Directive, which he said seems to be directed at avoiding use of those categories of data for discriminatory purposes.

"So what about replacing the extra grounds for processing of special categories of data with some explicit restrictions on the use of any data for discriminatory purposes?"

The privacy attorney for one of the largest energy companies in the world would like the EU to adopt Canada's approach of exempting business-contact information from regulation. "I would like to see the Directive to be limited to sensitive data only, with the definition perhaps expanded a bit to cover truly private information."

The privacy leader for one of Europe's largest financial institutions hopes that the EU will increase the specificity for how a data transfer is defining, excluding situations where people in non-EU locations only access data hosted in the EU.

Jacqueline Klosek, senior counsel with law firm Goodwin Procter, opined that "[t]he Directive

should establish more uniform rules regarding the meaning of "consent" that all EU countries will have to abide by."

4. Better reconcile privacy goals with other rights.

No respondent disputed Europe's ability to define privacy as a human right, a position that marks it as a leader worldwide. That said, some see the Commission routinely giving privacy a "trump card" over other long-established rights and social objectives.

Edward McNicholas, a partner with the privacy practice in the Washington, D.C. office of law firm Sidley Austin, stated that "the Directive should not inhibit corporate efforts to maintain compliance and integrity. It should provide clear and express authority for employer investigations of corruption, anticompetitive actions, improper workplace conduct, and other internationally-recognized wrongs."

The privacy leader for a large EU financial institution agreed. One change he hopes for is "hassle-free processing of personal data when necessary to comply with regulatory and legal obligations, including internationally, such as providing data to law enforcement cross border and conducting know-your-customer and anti-moneylaundering checks."

5. Improve enforcement.

Non-EU companies operating in Europe have noticed in the past two years an increase in some member states' enforcement of their data-protection laws. The EU DPAs as a whole had long been faulted for not enforcing the Directive, so this change generally is seen as a positive development.

Two CPOs of Fortune 100 companies see room for improvement in how the enforcement is carried out. Said one: "There is a perception, whether true or not, that the Directive is enforced in a manner that places greater restrictions on U.S. companies doing business in Europe than it does on European companies. Basically, we are held to a higher standard, with higher costs."

A Canada-based CPO believes that adding a breach-notification requirement to the Directive would equal the playing field. "Building in more notification and accountability will be steps in the right direction," he said.

As Canada, and now Australia, have completed reviews of their federal privacy laws, many are looking toward the European Union to do the same. The smooth functioning of global commerce—and the competitiveness of European companies—may well depend on it.