

Reproduced with permission from Privacy & Security Law Report, 10 PVLR 1430, 10/03/2011. Copyright © 2011 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

Getting a Grip on Filings With International Data Protection Authorities



By **LOTHAR DETERMANN** AND **DENISE LEBEAU-MARIANNA**

Multinational businesses have to overcome a number of hurdles in their strides to share personal data across geographies and keep all subsidiaries in compliance with data privacy laws in their respective jurisdictions.¹ One of the many compliance tasks is keeping up with government notification and authorization requirements. In this article, we provide an over-

¹ Regarding the three major compliance hurdles, see Lothar Determann, *International Data Transfers from Europe and Beyond*, 25 *Rev Bank Financ Serv* – 2009).

Prof. Dr. Lothar Determann practices data privacy, technology and international business law at Baker & McKenzie LLP (<http://www.bakernet.com>) in San Francisco / Palo Alto, and teaches Data Privacy, E-Commerce and Computer Law at University of California, Berkeley School of Law (Boalt Hall) and Hastings College of the Law (San Francisco), Freie Universität Berlin and Stanford Law School. Denise Lebeau-Marianna practices data privacy, IT, e-commerce and internet law at Baker & McKenzie SCP in Paris. The authors thank their Baker & McKenzie colleagues around the world for valuable contributions to this article, in particular Andrea Grubinger, Vienna, and Jordi Masdevall, Barcelona.

view and some practical recommendations, in particular with respect to requirements under French law.

1. Overview.

A significant number of European Economic Area Member States require companies to provide notice of some or all processing of personal data in filings to the data protection authorities. In some cases, companies have to obtain prior approval from the authorities. Similar requirements are increasingly appearing outside the European Economic Area, for example, in Argentina, Israel, Switzerland and Russia. The requirements vary significantly as to:

- the circumstances that trigger filing requirements (e.g., all automated processing, processing by more than a certain number of employees, processing of certain types of data, processing for certain purposes, international transfers, controller vs. processor activities, whistleblower hotlines, etc.),
- the degree to which the authorities provide guidance on the information that should be provided (some jurisdictions including Belgium, France, Spain and the United Kingdom offer online registration with restricted text fields or multiple choice questions; other jurisdictions require paper forms or allow free form notifications with respect to some or all required reports, e.g., updates),
- the amount and kinds of information to be provided,
- the extent to which companies have to notify and disclose information regarding onward transfers of data by the initial recipients,
- the extent to which exemptions apply to different approaches for justifying international data transfer to outside of Europe, e.g., EU-approved standard contractual clauses, EU/U.S. Safe Harbor certification, consent, etc.
- whether data transfer agreements or other supporting documentation must be submitted along with notification forms (authorities in some jurisdictions such as Austria, France, the Netherlands, Romania and Spain require submission of data transfer agreements where international data transfers are concerned; authorities in most other jurisdictions reserve the right to request supporting documentation at any point),
- whether controllers must specify the data processors, e.g., service providers, to which personal data are provided and to what extent,
- whether the filings must be translated to the local language (typically jurisdictions require filings to be

in the local language(s), although there are exceptions, e.g., in the Netherlands, data controllers may submit requests for data transfer permits to the Ministry of Justice in English),

- whether mere notification or prior approval is required regarding some or all aspects of data processing, and
- the penalties for non-compliance.

2. Examples.

A few country-specific examples illustrate the general points made thus far:

(a) European Jurisdictions.

In **Austria**, controllers must notify the data protection authority before any data processing activities may occur, unless such activities fall within narrow exceptions (e.g., certain business contact data; certain employee data with limited recipients); pertain only to published or certain public personal data, personal or family data processed for private purposes, or data relating to journalism; or, indirectly pertain to personal data. In some cases, controllers must seek formal approval from the authority, e.g., for implementing international whistleblower hotlines and transferring data outside of the EU even if justified by data transfer agreements incorporating EC-approved standard contractual clauses.

Data controllers that process personal data in **Belgium** are exempted from notification requirements if the processing pertains only to management of employees' wages, personnel or customers. However, this exemption does not apply where sensitive or evaluation data is processed, or when data is transferred to third parties—including entities in the same company group—unless the transfer is required by law. Approvals are generally not required, provided that cross border transfers to outside of the EEA are either covered by the recipient's Safe Harbor certification or data transfer agreements based on the appropriate Standard Contractual Clauses. As in the United Kingdom, the filing takes place online, although hard copy forms must be printed after submission, signed, and sent to the authority via mail.

In **Denmark**, data controllers must generally seek approval from the data protection authorities prior to transferring personal data to a non-EEA country. Transfers to Safe Harbor-certified entities, however, are exempt from these approval requests. Nevertheless, onward transfers to other recipients worldwide that are not Safe Harbor-certified require approval (even if there is an onward data transfer agreement that incorporates EC-approved standard contractual clauses or the data are non-sensitive). Obtaining written consent, on the other hand, would exempt controllers from the foregoing filing requirements.

German federal data protection law requires prior approval, unless the German company has appointed a data protection officer (which is mandatory anyhow for companies with more than nine employees involved in automated data processing)² and selects an EC-approved data transfer compliance mechanism for data transfers outside of the EEA, such as contracts based on

² L. Determann and C. Rittweger, *Legal Requirements and Options: German Data Protection Officers and Global Privacy Chiefs*, BNA's *Privacy & Security Law Report*, (10 PVLR 639, 4/25/11).

the Standard Contractual Clauses or an EU-U.S. Safe Harbor filing.³

There are general legal obligations in **Switzerland**, **Sweden**, and **Norway** to notify governmental authorities of data processing activities. As in Germany, such obligations are obviated, however, if the relevant controllers in those jurisdictions appoint a data protection officer.⁴ Unlike Germany, however, Switzerland, Sweden, and Norway require controllers to notify the data protection authorities of the data protection officer's identity to invoke the exception to the filing requirements. Naturally, this invites some degree of governmental scrutiny as to the statutory eligibility and appropriateness of the individuals appointed. While this can be done with a simple cover letter in Switzerland, Swedish and Norwegian controllers must submit an official one-page form to the government regarding the appointment.

In **Ireland**, both controllers and processors must generally register (either online or via a mail-in form) details about their processing of personal information, but only if they fall under certain categories, for example: bank and financial or credit institutions, businesses whose operations consist mainly of direct marketing, internet access providers, telecommunications network or service providers, or health professionals processing personal data related to mental or physical health, etc. As in the United Kingdom, registrations are added to a public register and there is no formal approval process aside from registration.

In **Italy**, companies do not have to notify international data transfers as such, but notifications are required for specific data processing activities that are deemed to pose risks for the protection of personal data (among others, profiling activities, processing of genetic data)⁵ and in connection with such notifications, companies also have to notify the Italian government whether they will transfer data outside the EEA.

In the **Netherlands**, controllers that justify international data transfers with data transfer agreements based on the EC-approved standard contractual clauses must undergo a two-part process to complete the notification process. They must first seek a data transfer permit from the Ministry of Justice. Provided that the permit is issued, controllers must then file a notification with the Dutch data protection authority.

In **Spain**, the data protection authority insists on prior government approvals where companies justify international data transfers with data transfer contracts, but allows companies to transfer personal data based on mere notifications (i.e., without seeking government approval) if the data subject granted consent

³ See Section 4(d) of the German Federal Data Protection Act, http://bundesrecht.juris.de/bdsg_1990/_4d.html (Deutsch) and http://www.bfdi.bund.de/EN/DataProtectionActs/DataProtectionActs_node.html (English, accessed Sept. 29, 2011).

⁴ See L. Determann and C. Rittweger, *Legal Requirements and Options: German Data Protection Officers and Global Privacy Chiefs*, BNA's *Privacy & Security Law Report*, (10 PVLR 639, 4/25/11).

⁵ Section 37 of the Italian Privacy Code (Legislative Decree June 30, 2003 n. 196 and following amendments and integrations). See, more generally, the website of the *Garante per la protezione dei dati personali* (the Italian Data Protection Authority): <http://www.garanteprivacy.it/garante/nav/jsp/index.jsp?solotesto=N> (accessed June 26, 2011).

or the recipient company registered for the EU-U.S. Safe Harbor.⁶

In the **United Kingdom**, non-exempt controllers have to notify the Information Commissioner's Office (ICO) of the processing of personal information by completing an online registration form, but only if it is carried out using computers.⁷ The ICO publishes some of these details in its online register of controllers, which is available for public inspection. Unlike some other European jurisdictions, the U.K. ICO generally does not require very detailed information about a controller's processing. Rather, its aim is to set forth a general picture of controllers' processing activities.

(b) Non-European Jurisdictions.

In **Argentina**, databases must be registered online in Spanish. The data protection authority recommends filing data transfer agreements so that it can review them for compliance. However, this is not required, and companies typically execute such agreements without filing them with the authorities.

Israel requires registration using mail-in forms of the following databases to the extent information stored therein does not pertain to Information⁸ that has been authorized to be publicly available: (1) databases including more than 10,000 data subjects; (2) databases containing Sensitive Information⁹; (3) databases including Information that was not delivered by the data subjects, on their behalf or with their consent; and (4) databases used for "direct marketing." Under special circumstances, the Israeli Database Registrar may require the registration of a database even if it does not meet any of the above criteria.

In **Russia**, any data processing must be notified to the relevant regional office of the data protection authority, the details of which are posted online at the federal register. Early in 2010, the Russian Federation passed new legislation on data security safeguards that introduced new, relatively onerous requirements to disclose various technical information and classify information technology systems. It is expected that most registrants will likely engage IT service providers to assist in the completion of the new registration forms due to the specialized knowledge required to address its technical aspects.

(c) Renewing or Amending Filings.

Whenever companies are faced with any changes to the previously notified information, they are generally required by statute to update their notices to data sub-

jects and government authorities. The method of updating governmental filings can vary depending on the circumstances. In France, for example, companies must typically file an official "modifying notification form"; but, when the extent of the modifications is not extensive, the CNIL has accepted relatively informal letters listing the changes.

EEA Member States have different enacted materiality thresholds and specific timelines regarding changes. For example, the Netherlands require notification from companies of changes regarding the name or address of the Dutch data controller within one week; other changes have to be reported annually and only if they are significant, for example, material changes to the purposes of the data processing, the categories of data subjects and data categories, recipients of data, planned security measures and transfers of data to countries outside the EEA.¹⁰ But, many national laws are ambiguous on exactly what updates must be notified and do not specify any de minimis exemptions or permissible delays regarding the notification of changes to data protection authorities. Indeed, Austrian legislation, in theory, requires any changes to data processing activities to be immediately notified if they affect the accuracy of that which was previously notified. In practice, some companies deal with the uncertainties by revisiting their notifications annually, especially in jurisdictions where there is an annual requirement to re-register anyway, for example, the United Kingdom and Ireland.

3. Sanctions for Non-Compliance.

Sanctions for not complying with filing requirements vary from country to country. Germany, for example, permits administrative fines of up to €50,000 (about \$70,650) for a private controller's violation of the duty to notify the data protection authorities of automated data processing activities absent any exception.¹¹ Similarly, in Austria, controllers that collect, process or transfer personal data without having fulfilled their obligations to notify the appropriate authorities may be subject to administrative fines up to €10,000 (about \$14,132).¹²

4. French CNIL Filing Requirements in Detail.

Following the high-level overview at the beginning of this article, we now turn to the French filing requirements in more detail:

The French data protection authority (CNIL) requires companies to complete very detailed forms and, in cases of international transfers, obtain the prior approval of the CNIL.¹³

⁶ The Spanish data protection authority explains some of its positions and administrative procedures in guidance available in English at https://www.agpd.es/portalweb/english_resources/regulations/common/pdfs/instruccion_1-2000_ingles_pdf.pdf (accessed June 26, 2011).

⁷ http://www.ico.gov.uk/Home/tools_and_resources/register_of_datacontrollers.aspx (accessed June 26, 2011).

⁸ "Information" is defined as details "regarding the personality of a person, his/her marital status, intimate affairs, medical condition, economical condition, professional qualification, ideas and beliefs."

⁹ "Sensitive Information" is defined as (1) Details regarding the personality of a person, his private personality, his medical condition, his economical condition, his ideas and his beliefs; (2) Information, which the Minister of Justice ordered, with the approval of the constitution, law and judgment committee of the Knesset.

¹⁰ Article 28 of the Dutch Data Protection Act; see also official guidelines for personal data processors, Article 4.2.5 (http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp.shtml (accessed June 11, 2011)).

¹¹ See Federal Data Protection Act § 43(3).

¹² See Federal Act Concerning the Protection of Personal Data §§ 17(1)-(2), 52(2).

¹³ Article 103 of the Decree No 2005-1309 of 20 October 2005, enacted for the application of Act No 78-17 of 6 January 1978 on Data Processing, Files and Individual Liberties (Amended by Decree 2007-451 of 25 March 2007), posted in English by the French data protection authority CNIL (<http://www.cnil.fr/fileadmin/documents/en/Decree%202005-1309.pdf>

A notification is due for each data processing purpose,¹⁴ but not for each software product used or database created. Thus, if a company uses different applications for talent management, mobility management, training, etc., and all for the purpose of Human Resource management, then these different databases may be covered by one declaration.

The French data privacy law makes a distinction between (i) data processing which may benefit from an exemption, (ii) those subject to a simplified declaration or (iii) a normal declaration and (iv) those subject to an authorization.

The rational behind these different regimes of filing is the following:

- A particular data processing activity may be exempted by decree if it constitutes a common practice among French companies and involves the processing of limited categories of data, e.g. payroll data and supplier data. Exemptions are subject to certain conditions and do not apply if data are transferred outside the EEA to a country that has not been formally recognized by the European Commission as providing an adequate level of data protection (for example, countries including Argentina, Canada, Israel and Switzerland have been found to offer an adequate level of protection, but not the United States).
- Data processing that is inherent to the activity of a company such as human resources management, security badge data processing, telephony data processing, client data processing, etc. is subject to a simplified notification since the processing of these data is necessary and not seen as affecting the rights and liberties of the data subjects. The simplified notification applies provided that the applicable conditions set forth in the simplified standard (including the transfer of data for limited purposes) are strictly satisfied. The advantage of the simplified notification is to limit the filing formality to a one page form whereby the company represents that its processing complies with the strict conditions set forth in the applicable simplified standard issued by the CNIL.
- If a company cannot or does not want to satisfy the conditions of the simplified notification standard, it must file a normal notification. The notification form is more detailed and requires information on the categories of data processed, the purpose of data processing, the categories of recipients, the data retention term for each category of data, the conditions of transfers and means of protection.
- French law requires companies to obtain a prior authorization from the authorities¹⁵ before they engage in data processing activities that are considered

accessed June 26, 2011). The CNIL has enforced the prior authorization requirements at least once, in a highly publicized case against a Tyco subsidiary in France, see, http://www.theregister.co.uk/2007/05/29/tyco_breaks_france_employee_data_rules/; <http://www.cnil.fr/vos-responsabilites/les-sanctions-de-a-a-z/actualite-sanctions/article/la-cnil-condamne-la-societe-tyco-healthcare-france-a-30-000-eurosdamende-pour-manque-de-cooper/> (accessed Sept. 30, 2011) (6 PVL R 759, 5/7/07).

¹⁴ Indeed, pursuant to the French Data Protection Act, article 23 II, “a unique notification shall be required for a data processing coming from a single entity for a single purpose (. . .).”

¹⁵ According to Article 25(4) of the French data protection act of 1978; for an English translation of said statute as well as official guidance from the French data protection authority, see <http://www.cnil.fr/fileadmin/documents/en/CNIL->

likely to present a risk to the data subjects’ rights and liberties, such as a processing which may exclude an individual from the benefit of a contract (e.g., data processing for purposes of anti-money laundering compliance), processing of biometric data and transfers of personal data outside the EEA in many instances. For certain categories of “high risk” processing, the CNIL has issued a single authorization process which defines the conditions in which an authorization may be granted (e.g., whistleblowing data processing, anti-money laundering for banks, etc.). The advantage of the single authorization is to limit the filing formality to a one-page form whereby the company represents that its processing complies with the strict conditions set forth in the applicable single authorization decree issued by the French authorities.

Regardless of the applicable formality (even if the processing benefits from the exemption) and even if the company has a data privacy officer, the company must comply with substantive French data protection law and satisfy a number of requirements established by French data privacy law, including the following:

- notice to data subject,
- limited data retention term as required by applicable law,
- organizational and technical security measures, and
- implementation of contractual measures to protect the data flows in the context of a transfer of data to an entity located in a country that does not offer an adequate protection.

The CNIL occasionally finds, pursuant to company audits, that companies file notifications without complying with substantive law or without accurately disclosing details relating to the processing activities. In a recent case, a company received a warning from the CNIL because it filed a notification that did not cover the actual purpose of the processing.¹⁶ Also the CNIL applied a fine of €30,000 (about \$42,392)¹⁷ to a French company for, among other things, an excessive data retention term (which was not the same as the one set forth in the notification) and the absence of notice to data subjects (in contradiction of the information provided in the notification). Filing notification or authorization forms with inaccurate information may be sanctioned in the same manner as the absence of any filing.

In practice, the CNIL often determines inaccurate notifications a posteriori in the context of its powers to control and investigate—and not a priori in the context of reviewing the notifications upon submission. The CNIL tends to investigate companies based on enforcement priorities that are published annually. For instance, in 2010 the CNIL targeted video surveillance and security badge systems. Also, the CNIL takes action based on complaints received from data subjects or work councils on behalf of employees. The CNIL occasionally follows up on newspaper articles.

During investigations, the CNIL may access all systems and data processed by a company. The CNIL will check whether the data processing controller is properly covered by an adequate notification and will identify if there is any discrepancy between the notification

[recommandations-whistleblowing-VA.pdf](#) (accessed Sept. 30, 2011).

¹⁶ CNIL, deliberation n° 2010-113, April 2, 2010.

¹⁷ CNIL, deliberation n° 2008-187, July 3, 2008.

filed and the conditions of the processing in place. Based on our experience, the CNIL is used to identify the following non-conformities during its investigations:

- a company fails to provide proper notice to data subjects,
- a company notifies of a limited data retention term but does not observe the retention limit in practice,
- data security measures are insufficient,
- a failure to legitimize international data transfers adequately, and
- companies do not respond adequately to data subjects who assert their right to access, correction or deletion of their data.

Depending on the CNIL's assessment of a company's overall compliance efforts, whether violations are first-time offenses, how the company cooperated during the investigation and how the company remedies compliance deficits, the CNIL may limit its actions to a mere warning or decide to sanction the company by imposing fines. So far, fines have been rarely dramatic (up to a €45,000 maximum (\$60,434)). However, the CNIL publishes its decisions on its official website and occasionally in press releases to state examples.

Prior to a decision to sanction, the CNIL usually gives companies a warning and opportunity to remedy the situation by a deadline, typically from 15 days to two months. For instance, in one case from 2010, the CNIL asked a company to file a proper a notification.¹⁸ In another case, a company was required, among other things, to justify the reason for which data concerning matters like family situation, age or dependant children were collected.¹⁹ In yet another case, a company was sanctioned because the purposes of data processing indicated in the notification to the CNIL did not match reality, security measures taken seemed insufficiently clear and data were transferred outside the EEA to a country that did not assure adequate safeguards without implementing a Data Transfer Agreement (DTA) or otherwise legitimizing the transfer.²⁰

In France, the French criminal code provides for a sanction of €300,000 (about \$424,208) and five years of imprisonment for the legal representative of a company. The sanction can go up to €1.5 million (about \$2 million) for companies. This sanction applies per infringement.

The CNIL may on its own apply the following sanctions:

- In case of a first violation, the penalty may not exceed €150,000 (about \$212,104).
- In the event of a second breach within five years from the date on which the preceding financial penalty becomes definitive, it may not exceed €300,000 or, in case of a legal entity, five percent of gross turnover for the latest financial year, within a maximum of €300,000 (about \$212,104).

The CNIL may issue a warning to a data controller who does not comply with the obligations of the act. It may also order the data controller to cease the breach within a time limit it determines. If the data controller

does not comply with this order, the CNIL may impose the following penalties:

- a financial penalty proportional to the gravity of the breaches committed and the profits obtained from the violation; and
- an injunction to stop the data processing activities at issue.

In case of urgency, where the processing or the use of processed data leads to a violation of the rights and liberties mentioned in the first Article of the French data privacy law, the commission may, after proceedings where both sides are heard:

- demand a suspension of the data processing, for a maximum period of three months;
- decide that some of the processed personal data shall be blocked, for a maximum of three months; and
- notify the Prime Minister so that he may, if necessary, take measures to stop the violation.

The Prime Minister must inform the CNIL of the steps he has taken within 15 days of receiving the notification.

In case of serious and immediate violation of the rights and liberties, the CNIL president may ask, in summary proceedings, the competent court to order any security measure necessary for the protection of these rights and liberties, applying a daily penalty, if necessary.

5. Practical Considerations.

Keeping up with the various, ever-changing local requirements can be a significant task, especially for companies with a large number of foreign subsidiaries and consumer businesses/data. Companies should consider implementing a process that ensures that relevant changes are reported to a central person in charge (e.g., the chief privacy officer, corporate counsel and/or a foreign corporate compliance administrator), who can then either update filings instantly (in case of particularly relevant changes, such as changes of address or implementation of new databases or processing purposes), or in certain intervals (e.g., at the time of an annual EU-U.S. Safe Harbor registration or quarterly privacy compliance re-assessments). Even smaller organizations usually benefit from creating a compliance binder to collect and monitor all the various compliance tasks and measures (such as filings, appointment of data protection officers, execution and maintenance of data transfer agreements, policies, vendor agreements, etc.). This will also help ensure that the information communicated to various local authorities is consistent to the extent global systems, processes and policies are concerned.

Consistent communication and concerted coordination by multinational companies will be increasingly important going forward. On Nov. 4, 2010, the European Commission issued a communication²¹ to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions that addressed potential reforms to the personal data protection framework in Europe. In that communication, the Commission stated that it will explore the possibil-

¹⁸ CNIL, deliberation n° 2010-232, June 17, 2010.

¹⁹ CNIL, deliberation n° 2007-374, Dec. 11, 2007.

²⁰ CNIL, deliberation, April 14, 2007.

²¹ "A comprehensive approach on personal data protection in the EU," available at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (last visited June 26, 2011).

ity of simplifying and harmonizing the current notification system, including a uniform EU-wide registration form. Clearly, if operating subsidiaries may all use the same form, then multinational companies should be able to compile and keep track of the information solicited in the forms more cost effectively. On the other hand, it will be important to ensure that the forms are submitted with a consistent level of detail and style, so

as to not raise any questions among the various data protection authorities. Indeed, the Commission's communication also addressed whether data protection authorities should coordinate their activities when confronted with cross-border issues, implying that a notification filed in one jurisdiction may receive more scrutiny in another in the future.