Data protection reform in Scandinavia


Lee A Bygrave

Throughout Europe, countries are in the process of overhauling their current data protection regimes in the light of the demands set down by the European Union’s 1995 Directive on data protection.1 This article gives a short account of the reform activity going on in the Scandinavian countries, each of which have recently issued draft Bills for new data protection laws.2 The Scandinavian legislative proposals are important to study not least because they provide early guidance on the way in which some European states can be expected to implement the EC Directive. It should be stressed, though, that final adoption of these proposals is unlikely to occur without some changes being made to both their form and content.

The draft Bills are also worthy of examination because they originate in countries that, on paper at least, have taken data protection seriously. Sweden, Norway and Denmark were amongst the first nations to enact data protection statutes; indeed, Sweden was the very first country to enact such legislation at national level.3 Norwegian and Danish data protection legislation was enacted in 1978.4 The regulatory regimes established pursuant to each of these statutes are relatively stringent and extensive. Accordingly, the proposed new data protection laws for Scandinavia can be expected to set a benchmark for what European governments regard as a high level of data protection, at least for the near future.

EU influence

Each of the draft Bills is heavily influenced by the EC Directive. That this is the case with respect to the Swedish and Danish proposals is scarcely surprising given that Sweden and Denmark are EU member states. Norway, however, is not an EU member state but is party to the 1992 Agreement on the European Economic Area (EEA). As such, Norway will only be legally bound to comply with the Directive when the latter is formally incorporated into the EEA Agreement. While incorporation has not yet taken place, it is expected to occur soon. Thus, the Norwegian legislative proposal has

---

1 Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter termed ‘EC Directive’).
3 See the Data Act of 1973 (Datalagen, 1973:289), fully in force 1.7.1974. This is not the only time Sweden has scored a legislative ‘first’. Sweden was also the earliest out in enacting legislation granting citizens a general right of access to government-held documents, this right of access being established already in 1766 in the Freedom of the Press Act (Tryckfrihetsförordningen).
been drafted with the aim of satisfying the Directive’s requirements.

Adoption of the EC Directive has not been the only catalyst for work on the draft Bills. Just as important has been a desire to overhaul old legislation in the light of new technological developments and new ideological concerns. At the same time, though, it is noteworthy that the draft Bills rarely make any attempt to improve upon the level of data protection stipulated by the Directive. Indeed, the committee responsible for drafting the Swedish proposal stated that it would have preferred to adopt a more liberal regulatory approach than the Directive embodies, in the sense that it would seek only to regulate those data-processing operations that involve ‘misuse’ of personal information.

National divergence

Although the committees charged with drafting the legislative proposals met each other on several occasions and took account of each other’s work, they made little attempt to arrive at a uniform Nordic platform on data protection. Concomitantly, they were all concerned to ensure that their proposals fit with their own national traditions. Thus, the draft Bills are similar mainly to the extent required by the EC Directive, and they differ – sometimes considerably – on many of the points where the Directive permits states a margin for discretion. The emergence of such differences already at this stage in the legislative process strengthens fears that the Directive is unlikely to realise its stated aim of bringing about equivalent levels of data protection across the EU.

Greater legislative detail

All of the proposals have been drafted as framework legislation that is to be supplemented by more detailed sectoral rules as the need arises. Compared to the current laws, however, the draft Bills contain more numerous and detailed substantive rules. They delineate more clearly the core data protection principle of ‘purpose specification’ or ‘finality’ (that is, personal data should be collected and processed for specified, legitimate purposes and not further processed in a way that is incompatible with those purposes). And, unlike the current laws, the draft Bills for Sweden and Norway (though not Denmark) each include an objects clause formally specifying the value(s) or interest(s) they are intended to serve.5

Licensing and notification

The general rule under Art 18 of the EC Directive is that data controllers need only notify data protection authorities of basic details of their intended processing operations. Some form of ‘prior checking’ by authorities is allowed pursuant to Art 20 but, from recital 54 in the preamble, it is

---

5 Of these clauses, the most instructive and innovative appears in the Norwegian draft Bill. The clause, as formulated by a majority of the committee responsible for the proposed law, reads: ‘The purpose of the Act is to aid in ensuring that processing of personal data occurs in accordance with fundamental data protection concerns, including the need for adequate data quality, personal integrity and privacy’. 
assumed that this will only occur in exceptional circumstances.

By contrast, the current data protection laws of Sweden and Norway operate to a relatively large degree with a requirement that data controllers seek permission (in the form of a license) from the national data protection authority before they establish a personal data register or engage in a particular data-processing activity. Some such licensing is also required under the Danish legislation but not to the same extent as under the Norwegian and Swedish Acts. Nevertheless, the regulatory regimes of all three countries focus the resources and attention of their respective data protection authorities on ex ante control of data-processing practices. These authorities devote relatively few resources to ex post facto auditing. Each of the draft Bills, however, envisage that ex post facto auditing will receive greater priority, at some expense to ex ante control.

In line with the EC Directive, the Norwegian and Swedish draft Bills cut back substantially on the licensing requirements of the current laws. The Norwegian proposal retains licensing only for the processing of especially sensitive data (as specified in Art 8(1) of the Directive) when the purpose of the processing is to make a decision that determines the legal rights/duties of the data subject. It also exempts data controllers from having to notify the data protection authority of (i) non-automated registers (unless these contain especially sensitive data) and (ii) the processing of publicly available data.

The Swedish proposal does not single out – at the level of statute – any specific data-processing operations in need of licensing, but makes provision for the government to stipulate – pursuant to regulations – licensing if necessary.

By contrast, the Danish proposal requires licensing with respect to certain categories of data processing by data controllers in the private sector. These categories include the processing of especially sensitive data (again, as listed in Art 8(1) of the Directive but also including data on ‘significant social problems’), processing for the purpose of so-called ‘black-listing’ (ie, warning persons against entering into business relationships with the data subject), and processing for credit-reporting purposes. With regard to data processing by public sector agencies, no licensing is required. In some cases, though, public sector agencies are not permitted to begin processing until after the data protection authority has given its opinion on the intended processing. This is the case, for instance, whenever a controller plans to carry out the matching of data for control purposes.

**Orientation of data subjects**

The current data protection laws of the three Scandinavian countries do not contain a general rule that data controllers must, of their own accord, inform data subjects about their data-processing practices. Under the influence of Arts 10 and 11 of the EC Directive, such a duty has been incorporated into each of the draft Bills. The Norwegian proposal goes even further than the Directive by including a duty of information when, on the basis of a personal profile, either a decision is made determining the data subject’s legal rights/duties or the data subject is approached/contacted. In such cases, the data subject must be automatically informed of the data controller’s identity, the data constituting the profile and the source of these data.
Regarding the information access rights of data subjects, the ambit of these under the current Scandinavian laws is largely limited to data held in computerised registers. By contrast, all three draft Bills – in conformity with Art 12 of the EC Directive – provide access rights irrespective of whether the information concerned is kept in computerised or non-computerised format.

The committees responsible for drafting the proposed new laws appear to have overlooked the practice of so-called ‘enforced access’. This is a practice whereby persons are pushed into utilising their access rights in order to provide a body on which they are dependent (eg, employer, insurance company) with personal information normally unavailable to the body. As it presently stands, Art 12 of the EC Directive fails to remedy this sort of practice clearly and directly. None of the three legislative proposals canvassed here confront this practice either.

Transborder data flows

With regard to regulating transfers of personal data to countries outside the EU/EEA (i.e., so-called ‘third countries’), the Danish and Norwegian draft Bills basically repeat what is contained in Arts 25 and 26 of the EC Directive. Nevertheless, some slight modifications are made. The Norwegian draft Bill specifies as a relevant factor for determining the adequacy of a third country’s level of protection whether or not the country has ratified the Council of Europe’s Convention on data protection. This factor, though, would be taken into account as a matter of course by other EU/EEA states even if it is not expressly mentioned in their own legislation or in Art 25 of the Directive. Further, the Danish draft Bill supplements Art 26(1) of the Directive by allowing transfer of data to countries with inadequate protection levels when the transfer is necessary for investigation or prevention of crime, and/or when the transfer is necessary to protect national security or public safety.

It is interesting to note that the explanatory memorandum for the Danish draft Bill states that the standards set by the Directive (as opposed to those adopted by Denmark pursuant to the Directive) will constitute the primary point of departure for measuring the adequacy of third countries’ data protection levels. Also noteworthy is that the memorandum interprets the criterion of adequacy as being met when transfer of data to a third country will not result in ‘significant reduction’ of the protection aimed at by the Directive.

The Swedish draft Bill prohibits, as a general rule, all transfers of personal data to third countries, but then lays down certain exemptions to this prohibition. These exemptions embody, in effect, what is laid down in Art 26 of the EC Directive, though go one step further by stipulating that data transfers will automatically be permitted to countries that have ratified the Council of Europe’s Convention on data protection. Interestingly, the draft Bill avoids any express reference to the adequacy criterion in Art 25 of the Directive, providing instead for the government to issue regulations that specify countries to which data may be transferred.

---

Legal/juristic persons

Under Norway’s current data protection legislation, data on private corporations and other legal/juristic persons are expressly protected to much the same extent as data on individual natural/physical persons (hereinafter termed simply ‘individuals’). Data on legal persons are also expressly protected under Denmark’s Private Registers Act but not its Public Authorities’ Registers Act; that is, the processing of legal person data by government agencies falls outside the scope of the Danish data protection regime. Even in relation to private sector data-processing practices, legal persons (as data subjects) are not provided with exactly the same rights as an individual: they do not enjoy a general right of access to information that other organisations keep on them; access rights are granted only with respect to information kept by credit reporting agencies. As for the situation in Sweden, the Data Act does not expressly protect data on legal persons though the latter are provided with limited data protection rights pursuant to two pieces of sectoral legislation: the Credit Reporting Act of 1973 (Kreditupplysningslag, 1973:1173) and Debt Recovery Act of 1974 (Inkassolag, 1974:182).

The EC Directive is silent on the issue of whether or not legal person data are to be expressly protected; thus, it is up to each state to arrive at its own decision on the desirability of such protection. The Norwegian draft Bill dispenses completely with express protection for legal person data on the grounds that (i) such protection has proven to be largely unnecessary under the current legislative regime, and (ii) the data protection interests of legal persons differ in fundamental respects from the equivalent interests of individuals. The Danish draft Bill takes much the same line, although retains express protection for legal person data with respect to credit reporting activities. It also makes provision for the ambit of such protection to be widened in the future if this should be found necessary in the light of technological developments. At the same time, it should not be forgotten that legal person data capable of being linked back to a specific individual will be regarded as ‘personal data’ pursuant to both draft Bills and the EC Directive. Data on small companies will often be of this character.

Technology-specific provisions

While the Scandinavian countries’ current laws focus to a considerable extent on establishment and use of ‘registers’ of personal data, the draft Bills – in line with the EC Directive – shift regulatory focus primarily to the ‘processing’ of data largely irrespective of the way the data are organised and largely irrespective of the technology used.

None of the draft Bills contain provisions that specifically address the processing of personal data over the Internet. Some consideration was given to the desirability of inserting Internet-specific rules (including rules stipulating use of the Internet for the operation of data subjects’ access rights and data controllers’ notification duties) but it was felt that such an option was premature, risky and would break with the approach taken by the EC Directive.

The Norwegian proposal includes rules dealing specifically with ‘electronic surveillance’ (defined
as ‘continuous or regularly repeated person surveillance with the aid of remotely controlled or automatically operational equipment’). The concept of electronic surveillance is sufficiently broad to cover operations in which personal data are not actually registered or stored (for example, on film). As a general rule, electronic surveillance may only occur if it is ‘objectively justifiable’ in relation to the controller’s field of operations. This criterion of objective justifiability is sharpened to one of ‘special necessity’ when the surveillance is directed at a location ‘regularly trafficked by a limited number of persons’ (for example, a workplace). In either case, adequate warning must be given about the surveillance measures. The data protection authority is also given competence to step in and prohibit surveillance that does not meet with the above rules.