Germany takes the lead on binding corporate rules

Christopher Rittweger and **Ilana Saltzman** explain how developments in Germany could provide multinationals with some useful indications on how to get their corporate codes of conduct approved by Europe's national data protection authorities.

Multinational organisations seeking to legitimise international data transfers within their organisation by reference to an internal policy, or corporate rules, may now be permitted to do so, on the basis of guidance issued in June by the Article 29 Working Party, the EU data protection advisory body. This article examines the Working Party's guidance and looks at the practical interpretation by the German data protection authorities (DPAs), which have expressly encouraged multinational organisations to adopt corporate rules.

EU DATA TRANSFER RULES

For the most part, transfers of personal data from the EU to third countries may be made only where the third country ensures an adequate level of protection. The European Commission has the authority, as do national DPAs, to authorise third countries as having adequate protection, but to date this authority has been exercised sparingly, and only a small handful of countries have made the grade.

Some exceptions to the general rule exist, but they are, by design, limited. In many cases, intra-group transfers of data are made in situations where the exceptions do not apply. In those circumstances, many multinationals have tried to rely on an alternative route under most EU countries' laws. Under this route, transfers can be made where the organisation demonstrates adequate safeguards with respect to personal data protection, including by way of contract.

In practice, however, large corporate groups have found this route onerous and unwieldy, and instead a trend has developed favouring the use of an intra-group 'policy' or 'code of conduct'.

The recent Article 29 document effectively endorses this route in principle, while also setting out guidance, both as to the content of intra-group codes (called 'binding corporate rules') and the procedures for organisations to adopt them. The guidance is expected to assist corporate groups to develop a practical route to compliance with EU data protection laws. To this end, it should also be noted that the German DPAs so far have given the green light to a number of corporate policies which may well have pan-European impact, as will be discussed below.

CORPORATE RULES - THE CONTENT

In its guidance, the Working Party sets out a number of requirements for binding corporate rules to be considered as providing adequate safeguards with respect to the protection of personal data.

RULES MUST BE BINDING

The Working Party considers that corporate rules need to be binding, or legally enforceable, in order to ensure adequate safeguards. Specifically, corporate rules need to be both "binding in practice" and "binding in law". To be "binding in practice" the members of the corporate group, as well as each employee within the group, must feel compelled to comply with the rules. To be "binding in law" the rules must enable enforcement by individual data subjects, by recognition of third party beneficiary rights (eg. by a third party beneficiary clause).

The German DPAs have considered it sufficient for corporate rules to be "binding in practice" if (a) the parent company of a multinational group adopts the corporate rules and declares them binding for all group companies, (b) the corporate rules are communicated to everyone within the multinational organisation, and (c) it is made clear that breach of the corporate rules will be penalised in accordance with applicable law.

In order to be "binding in law", the German DPAs require an undertaking from the multinational's entities in the EU/EEA that, in the event of a violation of the corporate rules by data importers outside the EU/EEA, data subjects will be treated as if an entity within the EU/EEA had committed the violation. In this way, national authorities and data subjects can bring claims against the local data exporter.

DATA PROTECTION COMPLIANCE

The use of binding corporate rules will not remove compliance obligations resulting from the core data protection principles, and the rules should contain provisions that expressly address these issues. The core principles may not be as fully understood by members of corporate groups in non-EU countries, so the rules should contain tailor-made provisions on the handling of personal data, as well as a reasonable level of detail in the description of the data flows and purposes of processing.

To this end, the German DPAs require all core data protection principles mentioned in the Working Party's earlier document on international data transfers (WP12) to appear within the corporate rules. Further, the German DPAs allow multinationals to achieve the required detail in description of data flows and purposes by means of frequently asked questions (FAQs). Finally, it is advisable in light of the experience of the German authorities to define certain core terms (such as 'personal data' or 'data controller') within the corporate rules in plain and intelligible language.

UNIFORM RULES

As corporate rules are (potentially) global, there should be no distinction made in their application. In practice, the rules must apply generally throughout the corporate group irrespective of the place of establishment of the members, or the nationality of the

individual whose personal data is being processed. Nonetheless, the Working Party recognises that while the rules should be consistently applied across the corporate group, they may legitimately differentiate between personal data originating in the EU and otherwise. For personal data not originating in the EU, the corporate group need not enable individuals to enforce rights in the EU (although the Working Party observes that provision of this right would be seen as a serious commitment to data protection requirements).

The German DPAs have signed off on corporate rules that make a distinction between data collected within the EU and elsewhere. Generally, the German DPAs allow for two different models of uniformity. A multinational can either (a) provide for a so-called 'piggyback' solution, whereby the applicable European law also applies after a transfer of personal data from within the EU/EEA to a country outside the EU/EEA, or (b) provide for the application of local laws applicable in the place of processing, so that the standards established by corporate rules apply in addition to local laws where the laws do not provide for an adequate level of data protection.

Given that many multinational organisations do not wish to export the strict rules applying within the EU/EEA to countries outside the EU/EEA, the second solution may seem more attractive to global players.

GUARANTEEING COMPLIANCE

The rules should introduce a system that guarantees awareness and implementation of the rules both inside and outside the EU. The corporate group must be able to demonstrate that the rules are known, understood and effectively applied throughout the group by employees, and that employees have received appropriate training and have requisite information available to them. The Working Party recommends that the corporate group should appoint appropriate staff with top-management support to oversee and ensure compliance.

To this end, the German DPAs require (a) the communication of the corporate rules (links on Intranet-sites to the rules are deemed sufficient), (b) the training of data handlers (especially outside the EU/EEA), and (c) the establishment of bodies within the multinational which are responsible for dealing with privacy issues.

AUDITS

The rules should provide for self-audits and/or external supervision by accredited auditors on a regular basis with direct reporting to the board of the ultimate parent. The rules should also indicate that cooperation with national DPAs may also require audits to be carried out by, or on behalf of, such authorities.

The German DPAs have signed off on corporate rules that contemplate the primary responsibility of internal auditors, which would need to be assigned to external auditors only to the extent that privacy matters cannot be adequately handled by the internal auditors.

COMPLAINTS HANDLING

The rules should introduce a system by which complaints are dealt with by a clearly identified complaint-handling department, and any data protection officer or complaint handler must have an appropriate level of independence in the exercise of their functions.

The German DPAs have found it sufficient if complaint handlers are independent from their local management with respect to data privacy issues. To this end, it seems advisable to establish a first contact for any privacy issues within the local entity (such as a data protection officer or local HR manager) and to afford the persons concerned to escalate complaints to an independent body within the multinational established to deal with such complaints.

COOPERATION WITH AUTHORITIES

The rules should contain clear duties of cooperation with DPAs so that individuals can benefit from institutional support. There should also be unambiguous undertakings by the corporate group that the group as a whole, and separately its members, will accept the audit requirements described above and abide by the advice of the competent DPA on any issues related to the interpretation and application of the rules.

To this end, the German DPAs have accepted a provision in corporate rules whereby both the exporting and importing entities would respect the relevant authority's advice to the extent that (a) the importer and exporter are granted due process, and (b) the authority's advice is legally binding.

REMEDIES AND COMPENSATION

The rules should indicate that individuals would benefit from the right to a judicial remedy or entitlement to compensation, and should also contain provisions on liability (described below)

Passing the German DPA test

Dr Hansjurgen Garstka, Berlin's Data Protection Commissioner explains the process by which he and the other Land (state) Commissioners approved the binding corporate rules (BCR) of companies like Daimler-Chrysler, Deutsche Telekom, and General Electric.

Dr Garstka said that there is a two step process for the Land Data Protection Commissioners' (which regulate the private sector) approval of companies' BCR programmes as being consistent with German law.

The first step is to accept that the controller provides adequate data protection safeguards by way of BCR for the transfers of personal data from the EEA. There are negotiations between the applicant and the Working Group for International Data Transfers, chaired by Dr Garstka. This agreement is then notified to the plenary session of the Duesseldorfer Kreis (the group of Land DPAs who coordinate their policies on the private sector).

The second step is the formal approval of data transfers on the basis of the BCR which has to be given by the Land authority in which the HQ of the company exporting the data is based. Regarding groups of companies like DaimlerChrysler, there may be several Land authorities with jurisdiction. But after the Duesseldorfer Kreis has acknowledged notification of the BCR, all the Land authorities give their approval without further examination and their approval, therefore, applies to the other Lander throughout Germany.

and jurisdiction aimed at facilitating the exercise of these rights by individuals.

The German DPAs have accepted that compensation rights of an individual for violations of the corporate rules generally apply only within the EU/EEA. They have also required undertakings from entities within the EU/EEA that, in the event of violations of the corporate rules by data importers outside the EU/EEA, data subjects will be treated as if the relevant entity within the EU/EEA had committed the violation. Again, this ensures that the national authorities and data subjects can bring claims against the local data exporter.

Liability and assets

The Working Party considers that the headquarters of the group (if in the EU), or the EU member of the group with delegated data protection responsibilities, should accept responsibility for, and agree to take the necessary action to remedy the acts of members of the corporate group outside the EU, and where appropriate, pay compensation for damages resulting from a breach of the rules by any member (or where damages were not claimed, but the data subject remains dissatisfied by the remedies offered under the rules' complaint mechanisms or a complaint to the relevant data protection authority).

The rules should also provide that individuals can choose to take an action in either the country in which the group member originating the transfer is located, or the country in which the EU group member with delegated data protection responsibilities, is located.

The group should attach to any original authorisation request (discussed below) evidence that the group headquarters (if in the EU), or the EU member of the group with delegated data protection responsibilities, has sufficient assets or insurance to meet compensation claims for breaches of the rules.

Transparency

In addition to complying with the information provision requirements of the EU directive and national implementing laws, corporate groups should be able to demonstrate that individuals are made aware that their personal data is being transferred legitimately to other members of the corporate group on the grounds of an authorisation (described below) based on the binding corporate rules.

Regulatory approval

The Working Party proposes the adoption of a coordinated procedure, under which companies may make a single application in one EU member state for authorisation of their data transfers. Such authorisation will then lead to the granting of permits by the DPAs in all other member states in which the group operates. This, however, would mean that prior to coming to a decision all DPAs of the relevant EU member states would have to sign off on the content of the relevant corporate rules.

An alternative, supported by the directive itself, would be to approach one member state authority initially, with a request for that authority's approval. If the approval is forthcoming, the relevant authority would then notify the European Commission and all other EU member states, in accordance with Article 26(3) of the directive. The remaining member states would then have the right to object to the approval, but would be bound by the European Commission's decision in this respect.

It is worth noting that the directive contains no details regarding this notification and objection procedure (including the periods to be followed). A note issued by the Commission does, however, seek to lay out some criteria for carrying out Article 26(3) notifications. According to this note, the Commission will endeavor to notify objections, if any, within three months of the date of issuance of the acknowledgment of receipt. One would assume, therefore, that the Commission would expect a similar timeframe to apply for other member states to voice any objections, and for the Commission then to come to a final decision within a relatively short timeframe.

The second approach outlined above would appear to be preferable, as it is led by the Commission which (unlike member states) has the authority to bind all member states in respect of the approval. Moreover, there is definite merit, where practicable in the circumstances, in initiating the approval process with a national authority already demonstrating practical experience - and, even more importantly, adopting a commercially receptive, if not sympathetic, stance on intra-group transfer and privacy issues generally and on the use of corporate rules specifically.

The German DPAs, in the light of their recent approvals of corporate policies, certainly meet these criteria.

Modifications

Companies may update their corporate rules without the need to apply for a further authorisation, provided:

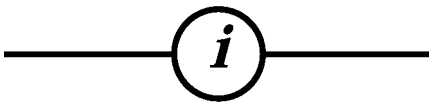
- no transfer of personal data is made to a new group member until the data exporter has ensured that the new member is effectively bound by the rules and can deliver compliance

- an identified person/department within the corporate group keeps a fully updated list of group members, and keeps track of, updates and provides the necessary information to data subjects or DPAs on request; and

- such updates to the rules, or changes to group members, are reported annually to the DPAs granting the authorisation with a brief explanation of the reason(s) for the update.

Where to now?

The Working Party guidance is encouraging for corporate groups seeking uniformity in their approach to global privacy compliance. Equally encouraging are the first approvals for data transfers obtained from German DPAs since they provide initial (and practical) guidance on the interpretation of the Working Group's requirements. Further, approvals such as those obtained in Germany may ultimately pave the way to a single 'one-stop-shop' approach to authorisation of data transfers - with a European Commission decision bringing finality to any individual member state approval, or any objection thereto - and ideally, also, some accepted forms of corporate rules which may come to be adopted as virtual standards across the EU.



AUTHORS: Christopher Rittweger and Ilana Saltzman are partners in the Munich and London offices of law firm Baker & McKenzie. They can be contacted by e-mail at: christoph.rittweger@bakernet.com and ilana.saltzman@bakernet.com.