# HOW VOLKSWAGEN MANAGES DATA PROTECTION AUDITING IN GERMANY

***Germany's new Data Protection Act (PL&B Dec'91 p.4) has meant some changes for data protection managers in Germany. Karl Theodor Weise, Data Protection Controller at Volkswagen for fifteen years, is responsible for data protection for 125,000 employees in six locations across Germany. He explains his view that whatever the legal regulations, the task of a data protection manager is always the same: safeguarding privacy and personal data. This German management model will also be of interest in other countries, even those which do not yet have a data protection law.***

The key word is *self-regulation.* This is not regarded as a way of avoiding data protection but as a proper means to involve those who are responsible for the processing of personal data and the protection of this data. Neither pure auditing nor pure administration will lead to efficient data protection: one can implement data protection only with, and not against, the people in charge of data processing. Especially in business, where frequent organizational changes are essential for successful operations, self-regulation is the natural way to meet these requirements.

### Role of the Company Data Protection Controller under Germany's Data Protection Act

The company data protection controller is a special feature of the German Data Protection Act, which encourages self-regulation. But self-regulation doesn't mean arbitrariness. In our data protection law, the company data protection controller is part of a multi-stage approach for implementing and auditing data protection.

The data processing staff have to respect the data protection laws when handling personal data. At Volkswagen we bind every office worker - whether he has to process individual data or not - by a written commitment and inform him about his and the company's legal obligations.

The company data protection controller has to implement data protection within the company in cooperation with the people mentioned before. Last but not least, the supervisory authority has an overall responsibility which includes very strict rights of auditing within companies and even the right to direct the company to adopt data security measures.

Perhaps we should remember that *it is the individual himself who is the first auditor of his data.* This perhaps is the kernel of data protection. In a world managed with computers, freedom of the individual is at stake. Uncertainty about the data in the possession of those big and medium sized brothers is the danger for individual freedom. Consequently, transparency of data processing is the most effective way to ensure this individual freedom. However the data protection organization is constructed, the individual must be supported in his role of controlling and auditing his own data. Data protection is not an end in itself.

So we get a *pyramid of control*: at the bottom there are literally millions of people processing the personal data of an unlimited number of individuals. They are mainly controlled by their supervisors. Data protection is an integral part of the duties of both of them.

In the next stage we find maybe thousands of internal data protection controllers organizing data protection within the company, and at the top of the pyramid there are some supervisory authorities. All of these have to serve the individual, who has the right to address his concerns directly to the supervisory authority.

### The Controller's Job as Envisaged by the German Data Protection Act

A company which processes personal data by computer and employs at least five employees permanently for this purpose has to

appoint a data protection controller. Of course, every company has to observe the data protection law, but there is no obligation to appoint a data protection controller at small companies. Where personal data is processed manually, the minimum number of people employed to do this before the appointment of a controller becomes necessary is twenty.

The data protection controller reports directly to top management. That does not mean that the controller's position is at the second highest level of management, but the law gives the data protection controller the right of immediate access to the top level of the company.

*The most important effect of this organizational set-up is the possibility of convincing top management to implement a good company data protection policy.* When top management has understood that a proper handling of personal data is an excellent way to ensure good relations with the people we work with, such as customers, this is half the battle.

The law states that only persons with the necessary knowledge and reliability may be appointed data protection controller. Of course, a broad knowledge is needed of data processing and of the data protection law and other legal provisions concerning personal data. A thorough knowledge of the company organization is also needed to work effectively.

Reliability is not only a question of character but of compatibility with other jobs. Only in big companies does the data protection controller have a full time job. In medium sized companies this task must be combined with other responsibilities. So conflicts of duty have to be avoided. *Imagine a manager responsible for personnel or for EDP who perhaps has to decide against the interest of either data protection principles or of company management.*

There is a legal provision that the data protection controller must not be subject to instructions from the management or anybody else in data protection issues. The management is not obliged to accept his opinion but in practice it does so regularly. The controller has the right of appeal to the government supervisory authority. *He should use this right from time to time in order to demonstrate to the company that he would not hesitate to use it when a serious matter may arise.*

## The VW Controller consults the DPA

An example. People write to us or telephone wanting information on new cars. Recently, Volkswagen contracted with another company to manage customer and other enquiries. This firm gathers data on these individuals. The data protection problem was whether these people have to be informed that their data, such as their address, was being processed by a company other than Volkswagen. This might cause some irritation.

Volkswagen management did not want to inform the data subjects. I thought that we did have to inform them. But the Lower Saxony Data Protection Authority decided that this company is only collecting data for Volkswagen. Under the new German law, this can be done by a written contract without giving further information to the data subjects. A consequence is that Volkswagen is responsible for the processing of the data, as long as it is carried out within the terms of the contract.

Although the supervisory authority agreed with the management on this occasion, it is good to have examples like this to show the management that the company controller has an active oversight role.

The law says that the data protection controller must not be placed at a disadvantage as a consequence of the performance of his duties. His appointment can only be cancelled on serious grounds or at the request of the supervisory authority.

The company has to support the data protection controller. The new law expressly details assistant personnel, rooms, equipment and funds. Most important is the implementation of a corresponding organization of auxilliary data protection deputies in the branches of a company. In a broad sense, everybody processing personal data must

regard himself as reporting directly to the company data protection controller (on data protection issues, of course).

### The Role of Employee Representatives

In Germany there exists a so-called Company Constitution Act, which includes some co-determination. This law states that the elected representatives of the employees have the duty to scrutinize the proper application of those laws which are to the benefit of the employees. The data protection law is one of these. The management must inform the employee representatives about plans affecting the processing of employee data and discuss these plans at a early stage. This influence is favourable for both the employee and the management. The individual employee may be afraid that his objection to the planned processing of his data would lead to reprisals by the company. On the other hand, the company is interested in consistent procedures as a basis for economic data processing. At Volkswagen, we do not process personal data without the consent of the works council, so we have never had a lawsuit on our hands. *The internal data protection controller is well advised to cooperate with these representatives.*

*The overall experience of company data protection controllers is positive.* That is not only my own impression. The position has been further improved by our new Data Protection Act, which has been in force since 1st June, 1991. In addition, internal data protection controllers have recently been installed by law in the social security institutions, and voluntarily in many other authorities.

### Working with the Data Protection Authority

In Germany, the Federal Data Protection Act is supervised by the state data protection authorities for the private sector. As we have seen, the concept of our law is cooperation and not confrontation between the data protection authority and the company data protection controller. The roles are different, of course: while the data protection authority is an independent state institution with the main purpose of supervising data protection, the internal data protection controller is mainly obliged to organize data protection within the company. Auditing is not his first duty.

### Legal Provisions Concerning the Relationship Between the Controller and the Authority

**Right of consultation** The company data protection controller has the right to consult the authority when in doubt about questions of data protection. One example is to seek confirmation of the legality of a planned personal data processing initiative. Data protection is a new field and there are many issues which are still controversial. It is helpful to have an official viewpoint in discussions with both the department which plans a certain personal data system and the individual who perhaps is not happy with the way his personal data is handled.

**DPA decision non-binding** The decision of the authority has no binding force, neither for the company, nor for the internal data protection controller, nor for the individual. The latter may apply to a court for a penal sanction or for *compensation for damages.*

**DPA right of investigation** The authority has the right to investigate the processing of personal data when there is a reason to assume that this processing is not in accordance with the law. But even then there are limited possibilities for changing the processing. But regularly the authority and the company find a way to take account equally of the individual's and the management's interests.

**DPA's right to require controller's replacement** Another legal provision is the right of the data protection authority to require the replacement of the company data protection controller if he lacks the necessary knowledge or reliability (this includes cases where he has additional duties in the company which may cause conflicts of interests). This right corresponds with the legal provision that the data protection controller cannot be replaced by the company, except at the request of the data

protection authority, or in cases of serious misconduct, or other substantial reasons.

In addition to these legal provisions, in practice the internal data protection controllers and the data protection authorities work together through *conferences* and similar forms of cooperation.

### Balancing personal data rights and protecting legitimate company interests

Data protection as a contribution to the freedom of the individual - who may be affected by the processing of data concerning him - is a concept which is well understood by business. Business is based on free enterprise and depends on free decisions of individuals to buy or not to buy, to cooperate or to refuse cooperation. There, business must cultivate a climate of confidence. Data protection is part of this culture, born from within and not from outside, rather a matter of codes than of legal restrictions. In this philosophy, self regulation is the appropriate way to achieve fair data protection within business.

*The internal data protection controller together with the supervisory authority guarantees a most favourable data protection, both for the individual and for the company.* No external authority is able to be in such a close and regular contact with the data processing in a company as the internal data protection controller. He knows the organization of the company very well, he is informed about new plans, he works together with this colleagues who are accountable for data processing and, last but not least, he liaises with the supervisory authority. He can thus effectively influence the way personal data is handled within the company in order to provide a good level of data protection.

*His first duty is safeguarding personal data.* But his good knowledge of the company's organization also enables him to achieve this in harmony with the legitimate interests of the company. In a manufacturing company, those interests concentrate on avoiding unecessary administrative overheads. Pure red tape cannot safeguard individual rights. On the contrary, *the image of data protection, and thus the respect accorded to it, is damaged by too much bureaucracy.*

There may be some concern about the costs, especially for those caused by the internal data protection controllers. Let me make two points on this:

1. Every company has to observe the legal provisions. A person specialised in this field obviously will find solutions which are more economic and will have a better chance of avoiding mistakes;
2. In most companies, the data protection controller does not perform this function full-time. The task is combined with others which are compatible, e.g. auditing or work in the legal department.

In Germany, we have found that the implementation of proper data protection has a valuable influence on the general organization of data processing. Data security requirements are likewise of interest to the company for financial or technical data, just as much as for data concerning the individual. Documentation is needed in every organisation.

### Company Data Protection Controller's legal responsibilities

In general, he has the duty to ensure that the provisions of the data protection legislation and other data protection policies are observed. This includes *assessing the legality of data processing*; organizing how to *guarantee* that *the rights of the individual* (for example, access to information on stored data concerning him) are observed; ensuring the *observance of confidentiality* on the part of all employees processing personal data; and *ensuring data security measures*, just to mention the most important issues.

### What the Law Emphasizes

- **supervising the processing of personal data.** For this purpose, company managers are obliged to inform the data protection controllers in good time about projects involving the processing of personal data.

- **informing the employees who process personal data about the data protection provisions** with particular reference to the situation prevailing in their department and the special requirements as to the protection of data arising from each departmental environment.
- **assisting and advising in the selection of persons to be employed** in the processing of personal data.

### Informing the Controller

Company management has to inform the internal data protection controller about the data processing equipment, the data files and their purposes, and the persons who have access to those files. As a rule, orderly system documentation is the best information, provided it includes those details which are relevant for data protection. There is no provision for registration of company data files with a supervisory authority in Germany (except for companies whose main business is the processing of sensitive personal data, for example, credit information).

To understand these different duties we perhaps should remember the underlying concept. For data controllers all men are potential evil-doers. But we divide these dangerous people into two categories: those who are not authorized to handle specific personal data, and those who are. The former group, of course, is the broad majority. It is our duty to keep them away from the data. Therefore, we implement adequate data security measures.

### Prevention of misuse of data

First it must be clear what the rules are. This includes the law and the company code of data protection.

Second we have to see that people perform their job in accordance with these rules. They include:

- selection of reliable people
- informing them about their duties
- making good data protection practice a contractual obligation
- supervising and auditing
- penalties.

The internal data protection controller has only an advisory role in the selection of those people who have to process personal data. Normally this is performed by formulating rules for the personnel department; they must be aware of the magnitude of the risks involved especially in data processing work.

### Motivating and Informing

Far more important is informing those employees who are authorised to handle personal data and who are in charge of processing it. Most important is the motivation of these people. This can be done best by reminding them that they are individuals too, who expect that their data will be handled properly. An indication as to penalties should be added.

Informing the employees in this way is a precondition for the undertaking which at Volkswagen has to be signed by every employee concerned.

### Auditing

Auditing data protection is a legal duty of the company data protection controller. We have to look at two quite different issues:

1. Future plans to process individual data
2. The current processing of this data.

The Data Protection Act emphasises the first issue. The reason is quite clear. Only at the planning stage do you have a real chance of influencing the system. When a system is in operation, a modification woud be so expensive that at least, you would face strong opposition, perhaps resulting in a bad compromise. Of course, significant failures must be corrected even if the costs are high.

For this reason the Data Protection Act not only obliges the data protection controller to audit the processing of personal data, but it adds that *the management has to inform the data protection controller about planned*

*systems sufficiently early so that he has a possibility of influencing the plan.* At Volkswagen all system concepts have to go through my office. So I am able to check whether there is individual data involved or not. *My experience is that people often do not regard data as individual data when this data is not sensitive.*

Systems already in operation have to be audited too. The special concern of data protection is observance of the legal provisions. In a big organization you will find an organizational structure of written and unwritten rules. In addition, the division of responsibilities guarantees a self-checking mechanism. Auditing of the operations concentrates on errors or violations, which needs very specialised knowledge. The data protection controller must be assisted by internal or external experts.

*Involvement of the auditing department* in the auditing of data protection has an additional benefit: when the role of the internal data protection commissioner is not regarded as a primarily auditing one, he will be more accepted as an adviser in order to approve data protection. It is important that people do not hesitate to ask the data protection controller when they are in doubt or if they have already made a mistake, without the fear that this would have further consequences than simply improving data protection.

### Personal Computers and the Law

An increasing proportion of data processing is done on personal computers and work stations. In this case, one person takes responsibility for the way the computer is used. Of course you would be able to cripple these facilities by hardware or software controls, but the result would be an end of personal computing.

At Volkswagen, we install a data protection information package on every PC which is started whenever you boot your PC. You are invited to read further information or to run your application. Part of this information is that we do not allow the processing of personnel data on a PC. Nobody is permitted to use a PC unless he has signed an undertaking to observe both the legal and the company data protection provisions. Offenders face disciplinary procedures.

### Conclusions

My experience is that it would be impossible to ensure effective data protection primarily by control measures. In a world where data processing is so widespread, that would ultimately lead to precisely the "Big Brother is Watching You" situation which data protection is intended to prevent. The data protection controller should not be a Big Brother.

We must keep in mind that *data protection is a part of good human relations*. The more we involve those who are responsible for processing personal data in the protection of this data, the more we will achieve good data protection. The internal data protection controller is an expression of this self-regulating responsibility which falls upon the processors of data.

Data protection in the data processing environment is a relatively new issue in law. We all have to learn from our experiences. Different approaches may enrich the fund of good data protection practices. But too many different laws would confuse the individual and would cause unnecessary costs to business. So there should be a steady development towards *a harmonization of data protection law* and towards an optimum of worldwide adopted principles which can be understood by everybody.

We need to legislate creatively to give us adequate instruments to properly serve the individual; keeping this in mind, the German approach is not of historical interest only, but a working example which is worth discussion at European level.

**This is an edited report of Herr Karl Theodor Weise's presentation at July's Privacy Laws & Business's 5th Annual Conference in Cambridge.**