

The necessity of company data security measures according to the Austrian Data Protection Act

28 August 2002

Dr Georg Röhnsner

E-mail: g.roehsner@lamberteversheds.com

Tel: +43 1 515 50

The words "data security" are today in every mouth. Owing to the rapid increase of data saving and particularly of e-commerce, data security will become one of the key issues for lawyers in the coming years.

Data are already today one of the most important business "commodity" and their importance will increase in the future in the same way, as the dangers, which are threatening individual from the data abuse, will do.

Last year Austria enacted a thorough new Data Security Act – The so-called "Data Security Act 2000" (hereinafter "DSA 2000") – which naturally follows very closely the relevant EU directives. It contains plenty of security regulations, which are widely unknown to an astonishingly large part of the population and above all the firms, which are representing a predominant part of data users. It surely plays a role that the sanctions provided for in the Act, were hardly imposed due to a lack of efficient administrative structures (and if this happens, than without appropriate publicity). With certainty we can assume, that this period of grace for "data sinner" will find its end in foreseeable time.

These explanations are not dealing with a "data abuse" – that it's prohibited, is generally wellknown (even if nobody knows in detail, what does it concrete mean) – but with another, until now extensively unnoticed aspect, which is not less important: **the obligation of data user to undertake satisfactory data security measures and the consequences, a violation of this obligation could bring.**

These data security measures let them divide into two big categories:

- the technical measures and
- the measures in connection to/with the employees (employment law measures)

Technical measures

Definitions:

Before we go closer into detail here, we should consider a few relevant definitions of the DSA 2000:

- **Data:**
Details about persons concerned (natural or legal person distinguished from mandator), whose identity is certain or ascertainable.
- **Mandator:**
Natural or legal persons, which have made the decision, to process (investigate, save, order, connect, interrogate, delete, ...) the data – no matter, if they do the proceedings by themselves or call on a third person for doing it.
- **Provider of services:**
who use the data, which were left to him for production of the work,

Who has to take the data security measures?

For all organisation's units of a mandator or service provider measures have to be taken to ensure the data security according S 14 DSA 2000.

This means, that **everyone (!), who uses the data**, is obliged by the Act, to take the appropriate measures for their security.

Which intensity of data security measures is provided for?

The Austrian data security act results from dynamic system of data security. This means, that the necessary amount of data security measures is not regulated in a uniform manner, but depends from the:

- type of used data;
- area and purpose of utilization;
- respective level of technical possibilities; and
- commercial liability.

This means:

- the trickier the used data are, the better they have to be protected (health data of natural persons or credit card's information need an essentially higher data security level in comparison to bare phone numbers...); and
- the data security measures have to be updated continuously in accordance to the technical development.

What have data to be protected from?

Data security measures have to guarantee, that the data:

- are secure from accidental or illegal damage and loss;
- are used properly;
- are not accessible to unauthorized persons.

Concrete measures

The act contains a catalogue of measures, that have to be set – along the requirements of the dynamic system "in particular":

- regulation of data and programs access rights, protection of data carrier from inspection and utilization through unauthorized persons;
- clear in-house regulation of data access rights;
- safeguarding of every set against unauthorized commissioning;
- regulation of admission rights of mandators or service provider to the premises;
- commitment of date utilization on valid orders of organisation` s units and co-workers, which are authorized to issue orders;
- management and saving (usually three years) of relevant protocol-data, for understanding the admissibility of manner of use;
- drawing up a satisfactory documentation of taken data security measures, to make the control and evidence protection easier.

But this catalogue is not conclusive – each measure going over it, which is necessary according to the circumstances of the case, for satisfactory insurance of the security level, is additional to be set!

Employment law's measures

Information of staff

Data security rules have to be enacted and available in such a way, that the affected members of staff can be at any time informed about regulations applying for them. All members of staff are express to be informed about obligations under the DSA 2000 or in-house rules and they have to be instructed in essential extent, too.

This instruction should be written (already in service contract, if possible) from the firm's point of view, because of the evidence arguments.

Contract obligations for preservation of data secrecy

Members of staff may transmit the data only on the basis of an express order of their employers. By transmission the DSA 2000 understands on the one hand the passing of data on to third persons or their publication, but also the utilization of data for any duty area of mandator other than that, for which the data original were compiled.

Mandator and services provider have to obligate their co-workers in contract (!), to transmit the data only by such a valid order and to keep the data secret even after the end of their work relationship.

Consequences of insufficient data security

Insufficient data security in the firm can naturally have – when it is used by a third side (by so-called "hacker") or it comes simply to data loss – pertinent commercial consequences. Loss of confidence by the clients, whose data were abused, or the costs of restoration of destroyed records are here named only as an example.

Nearby the regulations of the Act may also impose law consequences for such failure.

Administrative sanctions

An administrative sanction up to 9.445, - Euro by gross disregard for essential data security measures can be imposed by the appropriate regional office. The Administrative sanction proceedings will always be conducted against the responsible organs (commercial- or in the certain cases trade law secretaries, others on the basis of in-house structures persons having orders rights), because legal persons do not possess "criminal discretion".

Civil law liability

Yet the fundamentally higher thread is imposed by circumstances, which result from the possible civil law liability:

The relevant regulations of the DSA 2000 are representing measures with protective effect for third persons within meaning of S 1311 ABGB. By these we understand regulations, which prevent certain typical loss, which would be otherwise classified as "accidental". Who violates such a measures with protective effect for third persons, is liable for the resulting negative consequences, provided violation was culpable. For the assumption of culpability is light negligence suffices.

Should the firm alone not have enough EDP - competence, it should timely seek competent advice of a third undertaking to avoid later accusation of negligence.

If any loss occurs, because of a violation of data security regulations under the DSA 2000 (data loss, abuse by a third person, etc.), so the mandator or service provider is responsible for all third persons from the resulting loss. This may have – in the case of credit cards frauds on the basis of unsatisfactory data security in the area of an e-commerce - companies – ruinous dimensions.

This danger is still underestimated today by a lot of firms, everything, "concerning Computers", will be left from Management "to the EDP-freaks". But in the fact just the questions of data security should be the "Chief-matter"!

Besides a careful observation of relevant data security regulations, firms, which are administering the data an abuse of which may cause great financial loss should in any case provide for adequate insurance cover.

Copyright © 2002 Dr. Georg Röhsner, unless otherwise indicated. All information correct as at date of publication. Consistent with our policy when giving advice on a non-specific basis, we cannot assume legal responsibility for the accuracy of any particular statement. In the case of a specific problem, it is recommended that professional advice be sought.