

# e-commerce law & policy

**FEATURED ARTICLE**  
**09/09**



cecile park publishing

Head Office UK: Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND  
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com  
[www.e-comlaw.com](http://www.e-comlaw.com)

# Changes to privacy act: implications for e-commerce

The German Federal Council recently passed the 'Act on amendments to statutory data protection provisions', that enforces changes to the Federal Data Protection Act, the Telemedia Act and the Telecommunications Act as of 1 September. Dr. Jörg Hladjk, an Associate at Hunton & Williams LLP, examines the main areas for compliance under the Act from an e-commerce perspective.

The 'Act on amendments to statutory data protection provisions' of 14 August 2009, published in the Official Gazette No. 54 of 19 August 2009, p. 2854 et. seq. brought changes to the German Federal Data Protection Act, the Telemedia Act and the Telecommunications Act. Most amendments entered into force on 1 September 2009. They cover in particular encryption, security breach notification and service provider contracts. They also include new powers for data protection authorities and provide for increased fines for violations of data protection law provisions.

## Adjust marketing practices

The revised Federal Act introduces changes to the marketing rules. Depending on the business model, these rules may have to be taken into account by e-commerce companies in addition to the existing rules for e-mail marketing in the German Unfair Competition Act, and in addition to the existing provisions on the use of customer data and usage data in the German Telemedia Act.

Under the revised Federal Act, using contact details for marketing will be permitted only if the customer has expressly consented to such use. There are, however, certain exceptions:

- Processing and use of existing

data sets will continue to be governed by the old rules until 31 August 2012. During the transition period, the so-called 'list privilege' will continue to apply to previously collected data. The revised restrictions on processing and use of new data sets will apply from 1 September 2009 onwards.

● Consent will not be required for the processing and use of certain data combined in lists, provided that processing and use are necessary for one of the following purposes:

- promoting the e-commerce company's own offers if the e-commerce company collected the data directly from the customer or from a public directory;
- advertising regarding the professional services of a customer using a professional address.
- Data contained in lists may be transferred without the customer's consent provided that:
  - information regarding the origin and the recipient of the data is retained for two years; and
  - the advertisement identifies the data controller that originally collected the data.

In addition to taking into account the new rules when planning marketing campaigns, existing arrangements should be reviewed by e-commerce companies to evaluate whether there will be a legal basis for transfer and use of data after the 31 August 2012 compliance deadline.

## Implement encryption

The current annex to section 9 of the Federal Act requires that where personal data are processed or used automatically, the internal procedures of an organisation must be organised in a way that meet the specific requirements of data protection.

Although the current law already recognises encryption as an appropriate technical and

organisational measure, an amendment to the annex to section 9 of the Federal Act now explicitly refers to encryption tools and procedures as being appropriate for access control, admission control and safeguarding data transmission. Such encryption tools and procedures must reflect the 'Stand der Technik' (state-of-the-art technology).

From an e-commerce perspective, this amendment implies that all websites that collect personal data online via web forms or through other means should be reviewed in order to determine whether encryption has to be applied to protect data during the electronic transmission process.

## Develop security breach notification procedures

E-commerce companies will be subject to comprehensive breach notification requirements. From an e-commerce company perspective, the following categories of data are most relevant:

- bank or credit card account details; and
- customer data or usage data as defined in the Telemedia Act (e.g., data held by e-commerce companies, including registration or website usage data that may identify an individual user).

Notification is required in the event of unlawful data transfer or unauthorised access by third parties if the data loss is likely to have a serious impact on the rights or protected interests of the individuals concerned. The legislative commentary to the draft law indicates that both the types of data and the possible consequences of the breach should be taken into account when assessing whether the incident is likely to have a 'serious impact'.

Where notification is required, the data controller must notify the appropriate data protection

authority and the affected individuals without delay:

- after appropriate measures have been taken to secure the data; and
- once criminal prosecution will no longer be affected. The law also specifies certain minimum content requirements for the notification.

Where notification to individuals would be disproportionately burdensome, particularly where a large number of individuals are affected, notice must be provided to the general public. Such notification must be made by placing at least a half-page advertisement in daily national newspapers, or by other means that would provide equivalent exposure for the notification.

Failure to notify, notifying incorrectly, not completely or not in time, constitutes an administrative offence and can be sanctioned with a fine of up to €300,000.

E-commerce companies will therefore need to develop incident response procedures and to appoint an incident response team in order to ensure that any data breach is dealt with effectively, efficiently and in accordance with the legal notification requirements.

### Review service provider contracts

Under the new Act, contracts between e-commerce companies acting as data controllers and data processors such as entities providing call center services, electronic archiving services or data destruction services will need to contain detailed data protection requirements. The law lists ten issues that must be covered, including:

- scope and purposes of the data processing;
- security measures;
- data processor obligations;
- subcontracting rights; and
- audit rights.

Failure to conclude the contract

### These requirements will affect contracts between German entities as well as contracts between foreign service providers and their German customers

correctly, completely or not in the way as required, constitutes an administrative offence and can be sanctioned with a fine of up to €50,000. The same sanction applies in cases where the data controller does not assess compliance by the data processor regarding the technical and organisational measures taken by it, before the data processing begins.

These requirements will affect contracts between German entities as well as contracts between foreign service providers and their German customers.

### Review corporate data protection officer position

Corporate internal data protection officers employed by an e-commerce company will benefit from stronger employment rights under the new Act. The employment relationship may not be terminated by management without good reason, and termination is not permitted for at least a 12-month period after the term as data protection officer has come to an end, unless management is entitled to terminate based on important grounds. Data protection officers will also be entitled to participate in continuing education and training programs at the organisation's expense. Management should be aware of these changes to data protection officer employment status and may need to review current employment contracts or data protection officer appointment certificates accordingly.

### Understand new powers by data protection authorities

The amendments to the Federal Act also strengthen the powers of data protection authorities. The data protection authorities will be empowered to order e-commerce companies to remediate compliance failures, including deficiencies

relating to the collection, processing or use of personal data, or relating to technical or organisational measures. Where there are serious violations or deficiencies, the authorities will also be able to prohibit the collection, processing or use of data, or the implementation of individual data processing procedures, under certain circumstances.

### Create awareness of increase in fines and sanctions

The amendments to the Act also increase the maximum fines for failure to comply with data protection formalities from the current €25,000 per violation to €50,000, and from €250,000 per violation to €300,000 for more serious violations of the law. In addition, even higher fines may be imposed for commercial profits resulting from a violation - a violating company may be forced to disgorge profits that exceed the amount it would normally have to pay in fines.

### Conclusion

From adjusting marketing practices to implementing encryption measures, to renegotiating service provider relationships, and to complying with new data breach notification requirements, now is the time for companies to review their data protection practices and consider implementing a more holistic approach. To avoid business risks including fines, audits and reputational damage, compliance efforts must be properly focused. Data protection compliance and risk management must be understood as core elements of good business governance with respect to customers.

---

**Dr. Jörg Hladjk** Associate  
Hunton & Williams LLP, Brussels  
jhladjk@hunton.com

---



# cecile park publishing

Head Office UK Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND  
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com  
[www.e-comlaw.com](http://www.e-comlaw.com)

Registered number 2676976 Registered address 141 Wardour Street, London W1F 0UT VAT registration 577806103

## e-commerce law & policy

Many leading companies, including Amazon, BT, eBay, FSA, Orange, Vodafone, Standard Life, and Microsoft have subscribed to ECLP to aid them in solving the business and legal issues they face online.

ECLP, was nominated in 2000 and again in 2004 for the British & Irish Association of Law Librarian's Legal Publication of the Year.

**A twelve month subscription is £420 (overseas £440) for twelve issues and includes single user access to our online database.**

## e-commerce law reports

You can now find in one place all the key cases, with analysis and comment, that affect online, mobile and interactive business. ECLR tracks cases and regulatory adjudications from around the world.

Leading organisations, including Clifford Chance, Herbert Smith, Baker & McKenzie, Hammonds, Coudert Brothers, Orange and Royal Mail are subscribers.

**A twelve month subscription is £420 (overseas £440) for six issues and includes single user access to our online database.**

## data protection law & policy

You can now find in one place the most practical analysis, and advice, on how to address the many problems - and some opportunities - thrown up by data protection and freedom of information legislation.

DPLP's monthly reports update an online archive, which is an invaluable research tool for all those who are involved in data protection. Data acquisition, SMS marketing, subject access, Freedom of Information, data retention, use of CCTV, data sharing and data transfer abroad are all subjects that have featured recently. Leading organisations, including the Office of the Information Commissioner, Allen & Overy, Hammonds, Lovells, BT, Orange, West Berkshire Council, McCann Fitzgerald, Devon County Council and Experian are subscribers.

**A twelve month subscription is £390 (public sector £285, overseas £410) for twelve issues and includes single user access to our online database.**

## world online gambling law report

You can now find in one place analysis of the key legal, financial and regulatory issues facing all those involved in online gambling and practical advice on how to address them. The monthly reports update an online archive, which is an invaluable research tool for all those involved in online gambling.

Poker, payment systems, white labelling, jurisdiction, betting exchanges, regulation, testing, interactive TV and mobile gaming are all subjects that have featured in WOGLR recently.

Leading organisations, including Ladbrokes, William Hill, Coral, Sportingbet, BskyB, DCMS, PMU, Orange and Clifford Chance are subscribers.

**A twelve month subscription is £520 (overseas £540) for twelve issues and includes single user access to our online database.**

## world sports law report

WSLR tracks the latest developments from insolvency rules in football, to EU Competition policy on the sale of media rights, to doping and probity. The monthly reports update an online archive, which is an invaluable research tool for all involved in sport.

Database rights, sponsorship, guerilla marketing, the Court of Arbitration in Sport, sports agents, image rights, jurisdiction, domain names, ticketing and privacy are subjects that have featured in WSLR recently.

Leading organisations, including the England & Wales Cricket Board, the British Horse Board, Hammonds, Fladgate Fielder, Clarke Willmott and Skadden Arps Meagre & Flom are subscribers.

**A twelve month subscription is £520 (overseas £540) for twelve issues and includes single user access to our online database.**

- Please enrol me as a subscriber to **e-commerce law & policy** at £420 (overseas £440)
- Please enrol me as a subscriber to **e-commerce law reports** at £320 (overseas £440)
- Please enrol me as a subscriber to **data protection law & policy** at £390 (public sector £285, overseas £410)
- Please enrol me as a subscriber to **world online gambling law report** at £520 (overseas £540)
- Please enrol me as a subscriber to **world sports law report** at £520 (overseas £540)

**All subscriptions last for one year. You will be contacted at the end of that period to renew your subscription.**

Name

Job Title

Department  Company

Address

Address

City  State

Country  Postcode

Telephone  Fax

Email

**1** Please **invoice me**  Purchase order number

Signature  Date

**2** I enclose a **cheque** for the amount of

made payable to 'Cecile Park Publishing Limited'

**3** Please debit my **credit card**  VISA  MASTERCARD

Card No.  Expiry Date

Signature  Date

VAT No. (if ordering from an EC country)

Periodically we may allow companies, whose products or services might be of interest, to send you information. Please tick here if you would like to hear from other companies about products or services that may add value to your subscription.

priority order form

FAX +44 (0)20 7729 6093

CALL +44 (0)20 7012 1380

EMAIL [dan.towse@e-comlaw.com](mailto:dan.towse@e-comlaw.com)

ONLINE [www.e-comlaw.com](http://www.e-comlaw.com)

POST Cecile Park Publishing 17 The Timber Yard, Drysdale Street, London N1 6ND