

# e-Commerce

*Contributing editor*  
Robert Bond



2018

GETTING THE  
DEAL THROUGH

GETTING THE  
DEAL THROUGH 

# e-Commerce 2018

*Contributing editor*

**Robert Bond**  
**Bristows LLP**

Publisher  
Gideon Robertson  
gideon.roberton@lbresearch.com

Subscriptions  
Sophie Pallier  
subscriptions@gettingthedealthrough.com

Senior business development managers  
Alan Lee  
alan.lee@gettingthedealthrough.com

Adam Sargent  
adam.sargent@gettingthedealthrough.com

Dan White  
dan.white@gettingthedealthrough.com



Published by  
Law Business Research Ltd  
87 Lancaster Road  
London, W11 1QQ, UK  
Tel: +44 20 3708 4199  
Fax: +44 20 7229 6910

© Law Business Research Ltd 2017  
No photocopying without a CLA licence.  
First published 2000  
Fourteenth edition  
ISSN 1473-0065

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer-client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. The information provided was verified between June and July 2017. Be advised that this is a developing area.

Printed and distributed by  
Encompass Print Solutions  
Tel: 0844 2480 112



## CONTENTS

<b>The growth of outsourced solutions in data protection</b>	<b>5</b>	<b>Korea</b>	<b>58</b>
Janine Regan Bristows LLP		Kwang-Wook Lee, Keun Woo Lee and Jason Sangoh Jeon Yoon & Yang LLC	
<b>Brazil</b>	<b>7</b>	<b>Malta</b>	<b>65</b>
Raphael de Cunto, Pedro Paulo Barradas Barata and Beatriz Landi Laterza Figueiredo Pinheiro Neto Advogados		Olga Finkel WH Partners	
<b>Chile</b>	<b>13</b>	<b>Poland</b>	<b>74</b>
Claudio Magliona, Nicolás Yuraszeck and Carlos Araya García Magliona y Cía Abogados		Robert Małecki Małecki Pluta Dorywalski i Wspólnicy Spk	
<b>China</b>	<b>19</b>	<b>Portugal</b>	<b>81</b>
Jihong Chen Zhong Lun Law Firm		Leonor Chastre, Duarte Abecasis, Gonçalo Bastos Lopes, Mafalda Ferreira Santos and Paulo Costa Martins Cuatrecasas	
<b>France</b>	<b>27</b>	<b>Russia</b>	<b>88</b>
Bradley Joslove Franklin		Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva, Kseniya Lopatkina, Vasilisa Strizh and Brian Zimble Morgan, Lewis & Bockius LLP	
<b>Greece</b>	<b>37</b>	<b>Switzerland</b>	<b>95</b>
Dina Th Kouvelou and Nikos Th Nikolinakos Nikolinakos - Lardas & Partners LLP		Lukas Morscher and Stefan Bürge Lenz & Staehelin	
<b>India</b>	<b>45</b>	<b>United Kingdom</b>	<b>103</b>
Hardeep Sachdeva, Sunila Awasthi and Rachit Bahl AZB & Partners		Robert Bond Bristows LLP	
<b>Japan</b>	<b>52</b>	<b>United States</b>	<b>113</b>
Kozo Yabe and Takeshi Kanda Yuasa and Hara		Gregg Kirchhoefer, P Daniel Bond, Ashley Eisenberg and Adine Mitrani Kirkland & Ellis LLP	

# Poland

Robert Małecki

Małecki Pluta Dorywalski i Wspólnicy Spk

---

## General

### 1 How can the government's attitude and approach to internet issues best be described?

The Polish government strongly appreciates the importance of the internet. The significance of the internet, computerisation and digitisation has been emphasised by the creation in 2011 of a new ministry, the Ministry of Digitalisation, dealing with, inter alia, e-administration, information society and telecommunications.

---

## Legislation

### 2 What legislation governs business on the internet?

The following acts regulate business on the internet:

- the Civil and Criminal Codes;
- the Act of 18 July 2002 on the Electronic Provision of Services (AEPS);
- the Act of 5 September 2016 on Trust Services and Electronic Identification (ATSEI);
- the Personal Data Protection Act of 29 August 1997 (APDP);
- the Copyright and Neighbouring Rights Act of 4 February 1994 (the Copyright Act);
- the Telecommunications Law Act of 16 July 2004 (TLA);
- the Consumer Rights Act of 30 May 2014 (CRA); and
- the Act of 5 July 2002 on the Protection of Certain Electronically Provided Services based on, or consisting of, Conditional Access.

---

## Regulatory bodies

### 3 Which regulatory bodies are responsible for the regulation of e-commerce, data protection and internet access tariffs and charges?

These are matters for the president of the Electronic Communications Office (ECO) and Inspector General of Personal Data Protection. The president of the ECO is the regulatory authority for the telecommunications market, supervised by the Minister of Digitisation. The president of the ECO may, inter alia, impose financial penalties for breaches of the TLA and failure to observe its decisions. The Inspector General of Data Protection supervises personal data processing procedures and is authorised, inter alia, to impose administrative fines as coercion measures for breach of the APDP and failure to observe its decisions. The Scientific and Academic Computer Network (NASK) is a research institute responsible for the top-level '.pl' domain.

---

## Jurisdiction

### 4 What tests or rules are applied by the courts to determine the jurisdiction for internet-related transactions or disputes in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

The general principles referring to civil proceedings apply in such a case. In particular, the Lugano Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters of 30 October 2007, and European Parliament and Council Regulation (EU) No. 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters are of paramount importance.

If at least one of the parties is a resident of an EU member state, or of a country that is a party to the above-mentioned Lugano Convention, the parties may agree that a court in a particular member state shall have jurisdiction. Otherwise, persons resident in an EU member state should be sued before the courts of that member state, irrespective of their citizenship. In the case of a legal person, under the above-mentioned regulation the location of its registered office will determine the appropriate court, or alternatively the place of its main governing body or business activity. The claim may also be brought before a court where the obligation was or was to be performed.

As to agreements with consumers, the consumer may initiate proceedings against a legal person or an individual conducting business activity before the court having jurisdiction over its registered office or the place of the consumer's residence. Actions against a consumer may be taken by legal persons or individuals conducting business activity only in courts of the country where the consumer is resident.

If none of the aforementioned acts applies and there are no applicable bilateral agreements, the provisions of the Civil Procedure Code (CPC) apply. The parties may submit specific cases to the Polish courts, unless foreign courts have exclusive jurisdiction. The parties may also submit a given case to arbitration courts. In any case, Polish courts have jurisdiction if a contractual obligation was, is or was to be performed in Poland, the defendant is resident or has its registered office in Poland or the delict was committed in Poland. The place of performance of an obligation is not defined in the CPC: the Polish Supreme Court has ruled that the applicable material foreign law is to be respected when deciding on the place of performance of a given obligation. The same applies to the determination of the place of commitment of a delict. As regards contracts concluded by consumers, Polish courts have jurisdiction even though the other party, being a business entity, has its registered office abroad, if a consumer undertook the steps necessary for the conclusion of a given contract in Poland. Hence, if a consumer makes its declaration of intent in Poland, Polish courts will have jurisdiction even if the contract has not been concluded in Poland.

---

## Contracting on the internet

### 5 Is it possible to form and conclude contracts electronically?

**If so, how are contracts formed on the internet? Explain whether 'click wrap' contracts are enforceable, and if so, what requirements need to be met?**

Yes, it is possible. In the case of contracts formed electronically offline (email), an offer made electronically shall be deemed to have been made to the other person at the moment of its introduction to a means of electronic communication in a way that enabled that person to learn of its content.

In the case of a contract formed electronically online, an offer made electronically is binding for the offeror if the other party confirms its receipt without delay. This rule does not apply to contracts concluded by email and other means of individual long-distance communication. In business-to-business relationships the parties may agree on the exclusion of this rule as well. A party entering into a 'click wrap' contract should be provided with the terms and conditions of the vendor's contract. Moreover, the party that is a business entity should provide the other contracting party, inter alia, with information about technical acts covered by the execution of the agreement, the legal effects

of confirmation of the receipt of the offer and the languages in which the agreement may be concluded. If the contract is formed by email or another means of individual electronic long-distance communication, the general provisions of the Civil Code shall apply. In business-to-consumer (B2C) contracts, the business entity should also meet the additional conditions stipulated by the CRA.

According to the CRA, in business-to-consumer 'click wrap' contracts the entrepreneur is required to ensure that the consumer is fully aware of the obligation to make a payment after making an order under pain of the contract being regarded as unconcluded. If an order is made by clicking a particular 'button' on a website, such a 'button' should be described in a manner stipulated in the CRA. Moreover, the entrepreneur is obliged to ensure that the consumer is provided at the last moment before making an order with, *inter alia*, information on the main features of the product sold, price, extra fees (for example, fees for transport, mail service, other) or term of the agreement. The extra fees may be agreed upon by the consumer only by applying an 'opt in' option. Applying an 'opt out' option with regard to any extra fees releases the consumer from the obligation to pay for such fees. The entrepreneur is also obliged to provide the consumer with a confirmation of the conclusion of the contract at latest before the moment of providing the service or at the moment of providing a good. Such confirmation should be provided in a form of a durable data carrier which may be, for example, an email or a CD. Providing telecommunications services was made possible exclusively under a written agreement under the TLA. Since 21 January 2013, it has also been possible to provide such services under an electronically concluded agreement. The duration of an agreement for a specified period of time concluded with a particular consumer for the first time may not exceed 24 months.

#### **6 Are there any particular laws that govern contracting on the internet? Do these distinguish between business-to-consumer and business-to-business contracts?**

The general provisions of the Civil Code, the ATSEI and the AEPS also apply to internet contracts. B2C contracts are subject to provisions of the Civil Code and the CRA.

#### **7 How does the law recognise or define digital or e-signatures?**

Under Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation) and repealing Directive 1999/93/EC directly applicable since 1 July 2016, an e-signature means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign. The Regulation further defines an advanced e-signature as an electronic signature that meets the requirements of being uniquely linked to the signatory, capable of identifying the signatory, created using electronic signature creation data that the signatory can, with a high level of confidence, use under his or her sole control as well as being linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

#### **8 Are there any data retention or software legacy requirements in relation to the formation of electronic contracts?**

The Civil Code makes no such provision, but retention of such data is always in the interests of the contracting party in order to produce evidence in any subsequent proceedings.

Article 180(a) of the TLA requires public telecommunications operators or providers of publicly accessible telecommunications services to retain the transmission and localisation data generated or processed by those entities within the territory of Poland for 12 months and to make such data accessible to the competent authorities, including courts and prosecutors, on the basis regulated by special acts. These data do not relate to the content of contracts; they just confirm internet activity (time of log-in, IP number, etc). However, the Court of Justice of the European Union stated in its judgment of 8 April 2014 that Directive No. 2006/24/EC, being the basis for introducing data retention provisions into the TLA, is invalid as it interferes with the right to respect social life and the right to protect personal data. Such a decision may have an impact on the TLA provisions regarding data retention.

### **Security**

#### **9 What measures must be taken by companies or ISPs to guarantee the security of internet transactions? Is encryption mandatory?**

Under the APDP and AEPS, the data controller – being the data processor, including the service provider rendering electronic services – must take measures to ensure the protection of personal data that are subject to processing. The Regulation of the Minister of Internal Affairs of 29 April 2004 on documentation of personal data processing and technical and organisational requirements that should be met by personal data processing facilities and systems issued under article 39a of the APDP, provides (without prejudice to the rules set forth in the AEPS) most of the requirements for data processors consisting of three security levels – basic, higher and high. In those levels encryption measures are in some cases obligatory. For internet transactions encryption is obligatory as regards data used for verification of the identity of a person performing a transaction via the internet.

In addition, every provider of publicly accessible telecommunications services is obliged to notify the Inspector General of Personal Data Protection on any infringement of personal data and keep a register of infringements of personal data.

#### **10 As regards encrypted communications, can any authorities require private keys to be made available? Are certification authorities permitted? Are they regulated and are there any laws as to their liability?**

Under the ATSEI, qualified trust service providers are subject to entry into an open and electronic register kept by the Minister of Digitalisation upon the request of the aforementioned providers.

Pursuant to article 21(2) of the ATSEI, no liability is incurred by the trust service providers for any damage resulting from false data entered in the certificate that was provided by the recipient of trust services using that certificate unless the damage was a result of a lack of the trust service provider's due diligence. Qualified certification providers are subject to compulsory liability insurance.

Data for appending the e-signature (a private key) are only available to the person appending the signature, and there is no obligation requiring this person to disclose them. Additionally, other information related to the provision of certification services, including data used for verification of the authenticity of the signature and of the person (a public key) is confidential. However, it may be required by a court or a prosecutor if such information is connected with the pending proceedings, by state authorities when supervising the entities providing certification services and by other authorities empowered by separate acts.

### **Domain names**

#### **11 What procedures are in place to regulate the licensing of domain names? Is it possible to register a country-specific domain name without being a resident in the country?**

These matters are subject to the regulations of the registration body, NASK. In order to register a domain the interested party contracts with NASK. This interested party has to declare that the data it submits to NASK is accurate and that the submission of the offer and the performance of the contract does not infringe any third party's rights or the law. NASK does not examine whether by entering into or performing the contract the subscriber has infringed the third party's rights or the law. However, a final and binding judgment stating that a subscriber has infringed third-party rights may constitute grounds to terminate the contract. The interested party may also contract with private entities being NASK partners.

Moreover, depending on the particular matter, provisions concerning trademark protection, the Combating of Unfair Competition Act of 16 April 1993 (ACUC), copyright law and provisions of the Civil Code will apply. It is possible to register domain names without being resident in Poland.

#### **12 Do domain names confer any additional rights beyond the rights that naturally vest in the domain name?**

Generally domain names confer no additional rights, as registration of a domain means only that others may not hold this domain as their own. The 'first come, first served' principle applies in domain registration.



Industrial property law permits the registration of a domain as a trademark after the completion of specific formalities. However, use of a similar domain may constitute an act of unfair competition, especially where there is a risk that consumers will be misled as to the identity of the business holding the given domain.

### **13 Will ownership of a trademark assist in challenging a 'pirate' registration of a similar domain name?**

Trademark holders may sue a third party that is infringing their rights by using the domain name. Holders may demand that such use is stopped, as well as demand a reimbursement of profits gained by its use or the award of damages; a court may also order the defendant to pay a sum of money for charitable purposes. These claims can also be made against a person using a registered trademark as an internet domain.

## **Advertising**

### **14 What rules govern advertising on the internet?**

Advertising on the internet is not expressly regulated by Polish law. Therefore the general rules concerning advertising apply (ie, provisions of the ACUC, AEPS and regulations for the protection of incorporeal interests in intellectual property). In specific situations, the Press Law Act of 26 January 1984, the Gambling Act of 19 November 2009 and the Radio and Television Law Act of 29 December 1992 apply. In 2006 the Union of Associations Advertising Council was established, which is a self-regulatory body that oversees the practices of the advertising industry including entities that use the internet as a tool for advertising. The association adopted an Advertising Code of Ethics, which settles rules on advertising that protect the recipients as well as the beneficiaries of advertisements. The Advertising Ethics Commission is the body of the association that handles complaints from both consumers and competitors against entities that use advertising contrary to the Advertising Code of Ethics. The membership thereto is voluntary.

### **15 How is online advertising defined? Could online editorial content be caught by the rules governing advertising?**

Online advertising is not defined specifically in any legal act. The Radio and Television Law Act sets forth a definition of an advertisement as commercial information originating from a public or private entity in connection to its business or professional activity aiming at the promotion of sales or payable use of products or services as well as auto-promotion. Rules on banned advertising (see question 17) apply to online editorial content when such content may be recognised as advertising.

### **16 Are there rules against misleading online advertising?**

Under the AEPS, misleading advertising that may affect a client's decision as to purchase a product or a service constitutes an act of unfair competition. When assessing whether an advertisement is misleading all of its elements should be taken into consideration, in particular the quality and quantity of the elements of the good or service advertised, its manner of performance, usability, purpose and possibility of use, repair and conservation as well as the client's behaviour. There are no specific rules on the evidence that has to be kept by advertisers. The burden of proof that the information placed in an advertisement (or on the product) is true when it comes to civil claims under the ACUC lies on the advertiser, which is an exception from the general rule in civil law that the burden of proving a fact lies with the person who draws legal effects from that fact. In other claims connected to advertising, general rules of Civil (CPC) and Criminal Codes apply.

### **17 Are there any products or services that may not be advertised on the internet?**

Banned advertising, including advertising on the internet, includes: advertising contrary to the law, misleading advertisements, unjust comparative advertising, hidden advertising, advertising that invades privacy, spam and advertising of tobacco, alcohol (except for beer), psychotropic and abusive substances, games of chance and medicinal products that do not meet specific requirements.

Certain limitations apply to the advertising of medical services, services rendered by attorneys-at-law, notaries, as well as legal and tax advisers.

Total bans apply to content of a criminal nature, including child pornography, pornography with animals or content provoking crime, racial or ethnic hatred.

The provisions of the AEPS prohibit sending commercial information to natural persons that was not requested by them or sent to them without their consent. This restriction does not concern legal persons any more, which means that a company may receive unordered commercial information if it is not spam.

Nevertheless, the new provision of article 172 TLA introduced as of 25 December 2014 states that it is prohibited to use any telecommunication user's device (computers, smartphones, tablets, etc) or automatic system for the purposes of direct marketing (mailing) unless a user consents thereon. This provision protects consumers as well as business entities from receiving unordered marketing information. Failure to comply with the new rule may amount to a financial penalty imposed by the president of the ECO, up to the amount of 3 per cent of the income of the fined entity acquired in the previous calendar year.

### **18 What is the liability of content providers and parties that merely host the content, such as ISPs? Can any other parties be liable?**

See question 20 as to general rules of liability of content providers, entities providing hosting services and ISPs.

## **Financial services**

### **19 Is the advertising or selling of financial services products to consumers or to businesses via the internet regulated, and, if so, by whom and how?**

The sale of financial services products is subject to the AEPS, article 21 of the AFCBA and article 66(1) of the Civil Code. Service providers must provide the service recipient with information concerning themselves and the contractual procedure.

The CRA applies to consumers, who must be informed by the service provider about, inter alia, the identity of the service provider, the subject matter and conditions of the transaction, risks connected to the financial service (under certain conditions) and the right and method by which to withdraw from the agreement. The consumers' rights outlined in the CRA cannot be excluded or limited by the contract. Advertising of financial services products is subject to the requirements of fair advertising arising from the ACUC and the Act of 23 August 2007 on Counteracting Unfair Commercial Practices. This issue is also subject to regulations of the Polish Financial Supervision Authority.

## **Defamation**

### **20 Are ISPs liable for content displayed on their sites?**

A website's content provider or administrator, rather than the ISP, is generally liable for content displayed on the site. However, an ISP may be liable under civil law for any unlawful act as an accomplice of the tortfeasor.

An ISP that renders services consisting of transfer of data within a telecommunication network is not liable for its content if such an ISP is not the initiator of the data transfer, does not select the recipient of the data transfer and does not select or modify the information within the data transfer.

An ISP that renders hosting services (services that consist of making IT system resources available for storing data by the service user) is not liable for the content displayed on the site if it does not have actual knowledge of illegal information or activity, or upon obtaining an official notification or reliable information about the illegality of the given information or activity expeditiously disables access to the information.

### **21 Can an ISP shut down a web page containing defamatory material without court authorisation?**

If the web page clearly contains defamatory material, then the ISP which renders hosting services may shut it down without incurring liability for damages even without a court order, but after expeditiously informing the content provider of such an intent.

**Intellectual property****22 Can a website owner link to third-party websites without permission?**

Basically, yes. However, Polish law contains no explicit regulation concerning this issue and each case of linking should be considered individually, particularly with respect to the regulations of the Copyright Act and the Industrial Property Law Act of 30 June 2000.

**23 Can a website owner use third-party content on its website without permission from the third-party content provider? Could the potential consequences be civil in nature as well as criminal or regulatory?**

Under article 50(3) of the Copyright Act, making a work available to the public when and where the public chooses is one example of the fields of exploitation of the work, and this extends to the internet. The owner of the work rights may use and dispose of such work in all fields of exploitation.

The website owner may not display a third party's content that constitutes a work within the meaning of the Copyright Act without the express consent of the owner of the rights to that work.

However, the principles of permitted public use regulated by the provisions of the Copyright Act apply. In specific cases, a work can be used without the express consent of the copyright owner; however, this is without prejudice to his or her right to remuneration, if applicable. The consequences of unlawful use of a work may be of a civil as well as criminal nature under the Copyright Act as well as the Civil and Criminal Codes.

**24 Can a website owner exploit the software used for a website by licensing the software to third parties?**

Yes, if the website owner has copyright or licence rights to the software in the relevant exploitation field. If not, the copyright owner's consent is required.

**25 Are any liabilities incurred by links to third-party websites?**

Displaying a link to any unlawful content may result in joint liability in law if there was knowledge of the nature of the content. The entity displaying a link may also be liable if the link is classified as unlawful advertising or when the content or form of the link itself is contrary to law. So as not to be held liable, a given entity shall remove a link infringing law as soon as it receives an official or reliable information about the infringement.

**26 Is video content online regulated in the same way as TV content or is there a separate regime?**

The Radio and Television Act of 29 December 1992 sets forth different requirements and limitations to TV programme providers rendering their services through the internet as well as through standard means of TV signal transmission. Such entities are obliged to obtain a concession, or in case of programmes provided entirely through the internet, an entry to a special register in order to provide their services. As to misleading or prohibited advertising, or as to the use of works under the Copyright Act, the same rules apply to online TV programmes and online video content that is not a TV programme. Otherwise online video content and TV content are separate regimes.

**27 Do authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?**

In the Polish jurisdiction, IP addresses in some cases may be recognised as personal data, so in cases of IP infringement a civil procedure or a criminal procedure may be initiated resulting in a dawn raid or a freezing injunction.

**28 What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?**

Generally the rights and remedies under the Personal Data Protection Act are applicable thereto (they do not include search orders and freezing injunctions). However, in cases where IP infringement results in civil liability under the general rules of the Civil Code (for example, in cases of the breach of right to privacy, which is one of the personal

rights under article 24 of the Civil Code) a freezing injunction may be issued (see also question 38).

**Data protection and privacy****29 How does the law in your jurisdiction define 'personal data'?**

Under article 6 of the APDP, personal data is any information concerning an identified or identifiable natural person. An identifiable natural person is a person who can be identified directly or indirectly, in particular by identity number or by one or more specific factors determining his or her physical, physiological, intellectual, economic, social or cultural features. Information is not regarded as identifying where the identification requires an unreasonable amount of time, cost or manpower.

The APDP also regulates sensitive personal data as data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, party or trade-union membership, as well as the processing of data concerning health, genetic code, addictions or sex life and data relating to convictions, decisions on penalty, fines and other decisions issued by a court or through administrative proceedings. Processing and revealing those data is prohibited, except where the data subject has given its written consent thereto.

Under the APDP it is acceptable to use anonymisation to make data non-personal.

**30 Do parties involved in the processing of personal data, such as website owners, have to register with any regulator to process personal data?**

Pursuant to article 40 of the APDP, the data controller is obliged to notify a data filing system for registration to the Inspector General of Personal Data Protection, with the exclusion of data filing systems, inter alia, processed solely for the purposes of issuing an invoice, a bill or for financial reporting purposes, concerning persons enjoying medical or legal services, containing classified information or processed by particular public organs and others as set forth in article 43 of the APDP. A website owner is also released from the obligation of notifying data filing systems if it appointed a personal data security administrator, unless the data processed are sensitive or personal (such as data on ethnic origin, race, religious beliefs, etc). A data controller is the person who has real control over the processed data, and is not always the website owner.

The prior and explicit consent of the data subject is required for any sale of the data.

Pursuant to the APDP, a data controller may appoint an administrator of information security. However, the administrators of information security will be replaced by data protection officers according to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the GDPR), which will be directly applicable from 25 May 2018. Pursuant to article 37(1) of the GDPR, designation of a data protection officer will be obligatory, among other things, when the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale.

**31 Could data protection laws and regulatory powers apply to organisations or individuals resident outside of the jurisdiction?**

Subjects having their registered office residing in a third country, or that have their servers located outside the jurisdiction, in cases of the processing of personal data, are obliged to appoint a representative in Poland. Foreign subjects enjoy the same protection as national subjects.

**32 Is personal data processed on the basis of customer consent or other grounds? What is the commonly adopted mechanism for obtaining customer consent or establishing the other grounds for processing?**

The processing of personal data is based on customer consent. There are no formal requirements for obtaining customer consent, except in the processing of sensitive personal data (written consent). In the case

**Update and trends**

The GDPR is expected to have an impact on e-commerce in many respects. First of all, the new requirement of transparent and unambiguous consent for personal data processing, which is not to be assumed from inaction, will affect e-commerce significantly. Such consent must be specific and given by a data subject freely as a result of a separate request submitted in plain and clear language. Current consents may still be valid provided that they meet the new requirements. The responsibilities of data controllers will be extended, inter alia, by the obligation to notify the Inspector General of Data Protection of any data breach not later than within 72 hours from becoming aware of such a breach. Such an obligation is imposed on controllers regardless of the sector in which they operate.

of email and distance marketing in general, there are opt-in and opt-out requirements.

**33 May a party involved in the processing of personal data, such as a website provider, sell personal data to third parties, such as personal data about website users?**

In accordance with rules applicable to the processing of personal data, in Poland as well as other countries of the European Union, an unlimited sale of personal data is not allowed. The APDP does not prohibit the trade of personal data. However, the data subject must know about it and agree on the sale of its data. Information about to whom, for what purpose and to what extent the data is going to be transmitted should be communicated in such a way that the interested subject should be able to express his or her consent in a conscious way.

To the liability both for the seller and for the buyer, general rules of the Civil and Criminal Codes apply.

**34 If a website owner is intending to profile its customer base to carry out targeted advertising on its website or other websites visited by its customers, is this regulated in your jurisdiction?**

Yes, this matter is subject to the provisions of the APDP. In case of any breach of provisions on personal data protection, the Inspector General of Personal Data Protection may act ex officio as well as upon a motion of the person concerned.

Poland has introduced Directive 2009/136/EC of 25 November 2009 by amending the TLA to provide for an opt-in approach to the use of cookies. The user's consent to the use of cookies is always required, unless the use of cookies is necessary for enabling the use of a specific service explicitly requested by the subscriber or user or for the purpose of carrying out transmission of a communication via the internet. Before giving consent a user must be directly presented with clear and comprehensive information on the purpose and manner of using cookies, as well as on the option of using appropriate settings in its web browser or other application in a manner that disables cookies.

The user may consent to the use of cookies by accepting the aforementioned information presented to him or her by using the appropriate settings of a browser or other application.

Using cookies must not result in any negative effects on the user's software or hardware.

Although no legal acts or judgments on profiling have been passed in Poland it has been a subject of the GDPR, according to which 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements, etc.

**35 Does your jurisdiction have data breach notification or other cybersecurity laws specific to e-commerce?**

Yes, this matter is subject to the provisions of the APDP. In case of any breach of provisions on personal data protection, the Inspector General of Personal Data Protection may act ex officio as well as upon a motion of the person concerned. A data breach carries a penalty of a fine, penalty of restriction of liberty or deprivation of liberty for up to two years.

Furthermore, provisions of the AEPS establish obligations of a service provider related to providing services by electronic means and rules releasing service providers from legal liability concerning the provision of services by electronic means. This Act, as well as the APDP, also establishes rules for the protection of personal data of individuals using the services provided by electronic means.

**36 Does your jurisdiction recognise or regulate the 'right to be forgotten'?**

The right to remove all entries displayed in the contents of a web search engine is not regulated in our jurisdiction. This right has been recognised in the judgment of the Court of Justice of the European Union of 13 May 2014 (C-131/12).

**37 What regulations and guidance are there for email and other distance marketing?**

Email and distance marketing in general is regulated in the APDP, AEPS and the TLA.

Unsolicited marketing is not allowed. Email marketing relies on 'permission marketing'. A legal subject, which intends to send a newsletter or perform mailing has to ask the potential receiver for permission.

**38 What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?**

Generally the rights and remedies are regulated under article 32 of the APDP. Individuals have the right to control the processing of their personal data contained in the filing systems, especially to demand the data to be completed, updated, rectified, temporarily or permanently suspended or erased, in case they are not complete, outdated, untrue or collected in violation of the act, or in case they are no longer required for the purpose for which they have been collected.

In some cases unlawful personal data processing may also result in criminal responsibility or administrative fines under the APDP as well as civil responsibility under the general rules of the Civil Code.

These rights apply to citizens as well as foreign individuals.

**Taxation****39 Is the sale of online products subject to taxation?**

Yes, but the sale of products over the internet is not subject to separate tax provisions; online sales are subject to taxation on the same terms as ordinary sales. The issue is regulated by the Income Tax Acts, the Act on VAT and the Act on Civil Law Transactions. Within VAT taxation the Mini One-Stop Shop procedure is applicable to declare the VAT on online services provided to consumers.

**40 What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers within a jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?**

Regarding income tax, in certain circumstances this may result in the taxpayer having a permanent establishment in the given country and may result in liability for payment of income tax in that country on income generated in connection with the existence of such permanent establishment.

Placing a server in Poland does not influence VAT taxation on sales transactions. The nature of the transaction and the VAT taxation status of the purchaser are crucial to determine VAT liability.

**41 When and where should companies register for VAT or other sales taxes? How are domestic internet sales taxed?**

The place of registration should be the tax office competent for the company's registered office or principal place of business. Registration should be effected upon the commencement of business activities.

Internet sales are subject to general VAT rates applicable in Poland: the principal rate is 23 per cent and the reduced rate for some goods and services is 8 per cent. Certain goods and services are not subject to VAT (for further information, see question 39).



- 42 If an offshore company is used to supply goods over the internet, how will returns be treated for tax purposes? What transfer-pricing problems might arise from customers returning goods to an onshore retail outlet of an offshore company set up to supply the goods?**

The return of goods supplied over the internet is not subject to any particular tax provisions and should be settled according to general income tax and VAT procedures.

The taxation issues related to transfer-pricing provisions are not specifically regulated because of their internet character.

### Gambling

- 43 Is it permissible to operate an online betting or gaming business from the jurisdiction?**

This issue is regulated by the Gambling Act of 19 November 2009. According to its provisions, cylindrical games, card games, dice games and games on gaming machines may be provided only in physical casinos and bingo rooms. Organising online games of chance or online games on gaming machines is expressly prohibited. Operating an online mutual betting business is allowed but requires a licence. Pursuant to the amendment that entered into force on 1 April 2017 gambling operators who organise online gaming and own a licence or a permit or have notified such activity to a relevant authority are obliged to carry out payment transactions resulting from such gambling activity solely through payment service providers such as, inter alia, domestic banks or foreign bank branches. This requirement ensures adequate supervision of gambling-related financial flows resulting from the need for gambling operators to meet the requirements relating to money laundering and terrorist financing.

Furthermore, according to the amendment, the Minister of Public Finance maintains a register of domains used to offer gambling services illegally. The register consists of websites that operate online gambling without a licence, permit or notification to a relevant authority. As a result of placing the domain name in the register, access to the website is blocked and an adequate notification is displayed.

- 44 Are residents permitted to use online casinos and betting websites? Is any regulatory consent or age, credit or other verification required?**

Participating in online games of chance or online games on gaming machines is expressly prohibited by the Gambling Act of 19 November 2009. Residents who are at least 18 years old are permitted to use mutual betting websites. However, under article 107, section 2 of the Tax Criminal Code, it is prohibited to participate in a foreign game of chance or a foreign mutual bet within the territory of Poland. Anyone using such a service within Poland commits a tax offence subject to a fine.

### Outsourcing

- 45 What are the key legal and tax issues relevant in considering the provision of services on an outsourced basis?**

Outsourcing is classified and defined in the Council of Ministers' Regulation of 24 December 2007 on Polish Classification of Business Activity and in the Council of Ministers' Regulation of 4 September 2015 on Polish Classification of Goods and Services (with further amendments). There is no general regulation concerning the provision of services on an outsourced basis.

Special provisions for the banking sector are provided by the Act on Banking Law of 29 August 1997, which determines the conditions and principles that must be met in order to provide services on an outsourced basis. For example, the management and internal audit of a bank cannot be provided via outsourcing.

Tax law does not provide any special regulations on outsourcing. Therefore, the general provisions of Polish tax law are applicable.

- 46 What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation, do the rules apply to all employees within the jurisdiction?**

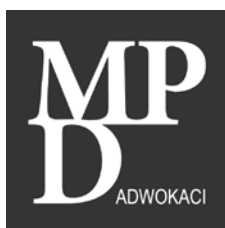
If outsourcing leads to the termination of employment contracts, the employer hires more than 20 people and a specific group of employees is made redundant, then under the Act of 13 March 2003 on Special Principles of Terminating Employment with Employees for Reasons Not Related to the Employees, the employer shall consult the trade union over such dismissals and is liable to make severance payments. However, this rule is applicable only where a trade union operates at the employing establishment.

In accordance with the Act of 7 April 2006 on Informing and Consulting Employees, if the employer hires at least 50 people, it shall inform and consult the employees' council on issues related to changes in the structure and operation of the business before using an outsourced company.

### Online publishing

- 47 When would a website provider be liable for mistakes in information that it provides online? Can it avoid liability?**

The Constitution of Poland, the Civil Code, the Press Law Act as well as international acts of law such as the Convention for the Protection of Human Rights and Fundamental Freedoms, provide for the right of freedom of speech as long as it is not prohibited by law. A website provider (being a content provider) is liable for the information displayed online under the general principles of the Civil and Criminal Codes or for infringement of other rights (eg, intellectual property rights or APDP). The content provider may be liable for publishing erroneous information on a website if the information infringes personal rights, causes damage or is in any other manner unlawful, and guilt for the unlawful result of publishing such information may be attributed to the content provider. The general principles of liability refer also to press



**Robert Małecki**

**rmalecki@mpd.com.pl**

Ul. Świętojerska 5/7  
00-236 Warsaw  
Poland

Tel: +48 22 828 14 60  
Fax: +48 22 827 04 63  
www.mpd.com.pl

published online. The author, editor, publisher and other persons that procure publishing of information are liable for the effects of publishing thereof.

The chief editor is obliged to publish a correction of inaccurate or untrue information within three days of receiving a motion of a person or entity. Business entities selling products via the internet may be liable for physical and legal defects of the goods sold to consumers and business entities. If the goods do not conform with the information provided to the contracting party the business entity may be obliged to replace the good or repair it, or either return the part of the price proportional to the extent of the defect or return the whole price paid by the contracting party if it withdraws from the contract. Business entities selling products via the internet may also bear civil or criminal liability for publishing misleading information on their services or products or providing false advertising.

**48 If a website provider includes databases on its site, can it stop other people from using or reproducing data from those databases?**

The Databases Protection Act of 27 July 2001 applies. A website provider that has a right to a database may prohibit unauthorised third parties from the total or partial use of such a database.

However, it is permitted to use part of a database made available on a website, which is not substantial qualitatively or quantitatively. Moreover, such use should not infringe the normal use of the database or harm the interests of its owner.

In any event, use of the database is permitted if the third party uses it for didactic or research purposes and identifies the source, or if such use is justified for a non-commercial goal, or for internal security and court or administrative proceedings. Nevertheless, recurring and systematic downloading or secondary use of the database is not permitted if this is contrary to normal use and results in unjustified violation of the owner's interests.

If the database can be regarded as a work according to the provisions of copyright law, the Copyright Act will additionally apply.

## Getting the Deal Through

Acquisition Finance  
Advertising & Marketing  
Agribusiness  
Air Transport  
Anti-Corruption Regulation  
Anti-Money Laundering  
Arbitration  
Asset Recovery  
Automotive  
Aviation Finance & Leasing  
Banking Regulation  
Cartel Regulation  
Class Actions  
Commercial Contracts  
Construction  
Copyright  
Corporate Governance  
Corporate Immigration  
Cybersecurity  
Data Protection & Privacy  
Debt Capital Markets  
Dispute Resolution  
Distribution & Agency  
Domains & Domain Names  
Dominance  
e-Commerce  
Electricity Regulation  
Energy Disputes  
Enforcement of Foreign Judgments  
Environment & Climate Regulation  
Equity Derivatives  
Executive Compensation & Employee Benefits  
Financial Services Litigation  
Fintech  
Foreign Investment Review  
Franchise  
Fund Management  
Gas Regulation  
Government Investigations  
Healthcare Enforcement & Litigation  
High-Yield Debt  
Initial Public Offerings  
Insurance & Reinsurance  
Insurance Litigation  
Intellectual Property & Antitrust  
Investment Treaty Arbitration  
Islamic Finance & Markets  
Labour & Employment  
Legal Privilege & Professional Secrecy  
Licensing  
Life Sciences  
Loans & Secured Financing  
Mediation  
Merger Control  
Mergers & Acquisitions  
Mining  
Oil Regulation  
Outsourcing  
Patents  
Pensions & Retirement Plans  
Pharmaceutical Antitrust  
Ports & Terminals  
Private Antitrust Litigation  
Private Banking & Wealth Management  
Private Client  
Private Equity  
Product Liability  
Product Recall  
Project Finance  
Public-Private Partnerships  
Public Procurement  
Real Estate  
Restructuring & Insolvency  
Right of Publicity  
Securities Finance  
Securities Litigation  
Shareholder Activism & Engagement  
Ship Finance  
Shipbuilding  
Shipping  
State Aid  
Structured Finance & Securitisation  
Tax Controversy  
Tax on Inbound Investment  
Telecoms & Media  
Trade & Customs  
Trademarks  
Transfer Pricing  
Vertical Agreements

Also available digitally



# Online

[www.gettingthedealthrough.com](http://www.gettingthedealthrough.com)



e-Commerce  
ISSN 1473-0065



THE QUEEN'S AWARDS  
FOR ENTERPRISE:  
2012



Official Partner of the Latin American  
Corporate Counsel Association



Strategic Research Sponsor of the  
ABA Section of International Law