e-Commerce 2020

Contributing editor
Robert Bond

LEXOLOGY®
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development managers
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 3780 4147
Fax: +44 20 7229 6910

First published 2000
Sixteenth edition
ISBN 978-1-83862-138-4

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

e-Commerce
2020

Contributing editor
Robert Bond
Bristows LLP

Getting the Deal Through is delighted to publish the sixteenth edition of e-Commerce, which is available in print, as an e-book, and online at www.gettingthedealthrough.com.

Getting the Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Getting the Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes a new chapter on Croatia.

Getting the Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.gettingthedealthrough.com.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Getting the Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editor, Robert Bond of Bristows LLP for his continued assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
July 2019

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2019
For further information please contact editorial@gettingthedealthrough.com

Contents

Brazil 3
Raphael de Cunto, Pedro Paulo Barradas Barata, Beatriz Landi Laterza Figueiredo, Luís Antônio Ferraz Mendes and Ana Carolina Fernandes Carpinetti
Pinheiro Neto Advogados

Chile 13
Claudio Magliona, Nicolás Yuraszeck and Carlos Araya
Magliona Abogados

China 22
Jihong Chen
Zhong Lun Law Firm

Croatia 34
Irina Jelčić, Iva Burić and Paula Jagar
Hanžeković & Partners Ltd

India 42
Hardeep Sachdeva and Priyamvada Shenoy
AZB & Partners

Indonesia 53
Fahrul S Yusuf and Mohammad K Bratawijaya
SSEK Legal Consultants

Japan 61
Kozo Yabe and Takeshi Kanda
Yuasa and Hara

Malta 69
Olga Finkel, Robert Zammit, Erika Micallef and Nicole Sciberras Debono
WH Partners

Norway 81
Jeppe Songe-Møller, Kaare M Risung, Trond Larsen, Øivind K Foss and Marie Berggren Hagberg
Advokatfirmaet Schjødt AS

Poland 91
Robert Małecki and Jan Wiegner
Małecki Pluta Dorywalski i Wspólnicy Spk

Russia 100
Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva, Kseniya Lopatkina, Vasilisa Strizh, Kamil Sitdikov and Brian L Zimbler
Morgan, Lewis & Bockius LLP

Switzerland 110
Lukas Morscher and Nadja Flühler
Lenz & Staehelin

United Kingdom 122
Robert Bond
Bristows LLP

Norway

Jeppe Songe-Møller, Kaare M Risung, Trond Larsen, Øivind K Foss and Marie Berggren Hagberg
Advokatfirmaet Schjødt AS

LEGAL AND REGULATORY FRAMEWORK

Government approach

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

The government acknowledges the internet as an integrated and natural part of Norwegian society and its business community, and has incorporated EU legislation relating to internet regulation, such as the InfoSoc Directive and the Audiovisual Media Services Directive. However, the pace of new legislation still lags behind the rapid development of online products and services, with issues such as the lack of effective countermeasures against online sales of illegal products and services from foreign websites to Norwegian consumers posing challenges for Norwegian courts and legislators. Consumer protection and data protection are prioritised by the Norwegian authorities, and the government has taken an active role in promoting the building of internet infrastructure and regulating commercial transactions. The consumer authorities have, in the past year, been particularly active in cross-border matters in conjunction with other European consumer authorities.

Legislation

2 | What legislation governs business on the internet?

Business on the internet is mainly governed by general business legislation, such as the Contracts Act and the Sale of Goods Act. Particular legislative attention has been paid to business-to-consumer sales, with several acts granting rights to consumers and imposing obligations on businesses dealing with consumers; and these also include provisions specifically relating to online sales. Of particular importance are:

- the Consumer Purchases Act;
- the Cancellation Act; and
- the e-Commerce Act.

Significant parts of Norwegian legislation governing business on the internet consist of implementations of EU directives and regulations through Norway's membership of the European Economic Area. Examples include:

- the InfoSoc Directive;
- the e-Commerce Directive;
- the Audiovisual Media Services Directive;
- the Distance Selling Directive; and
- the eIDAS regulation.

Regulatory bodies

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

The Norwegian Communications Authority monitors the technical side of e-commerce, such as the use of e-signatures. The Norwegian Consumer Authority monitors compliance with consumer rights and has explicitly stated that it targets, among others, e-commerce, digital terms, internet, telecommunications and television (TV), and the sharing economy. The Norwegian Data Protection Authority is responsible for overseeing data protection.

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?

Norwegian legislation does not explicitly regulate jurisdiction for international online sales. The choice of venue must therefore be decided using general principles of jurisdiction. The parties may choose the venue through agreement, unless the dispute is subject to mandatory provisions concerning exclusive jurisdiction. Norway is party to the Lugano Convention 1988, pursuant to which a case against a foreign seller of goods based in another convention state to a Norwegian customer must be brought before the courts of the seller's domicile. Several exceptions apply – such as, for example, the seller must be directing its business towards Norway or, provided that the customer is a consumer, the contract must be fulfilled in Norway. In these cases, the customer may bring the case before the Norwegian courts. If the seller is not based in a convention state, the conclusion depends on which conventions apply, but the general rule is that cases against the seller must be brought where the seller is domiciled. In any case, pursuant to the Disputes Act, the case must have 'a sufficient connection to Norway'. A dispute that might otherwise be brought before Norwegian courts could therefore be rejected due to a lack of connection, and vice versa; a dispute that might otherwise be rejected by the Norwegian courts could be accepted because it has a particularly strong connection to Norway.

Establishing a business

5 What regulatory and procedural requirements govern the establishment of digital businesses in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

There are very few regulatory and procedural requirements to establish digital business in Norway. Services defined as electronic communication services to the public may be subject to registration with the Norwegian Communications Authority. Otherwise, the regulation is on the content of the services and not on the establishment of the business as such. There are no restrictions on foreign ownership, but at least 50 per cent of the members of the board must be EEA citizens and reside in the European Economic Area. Non-Norwegians must obtain a D-number, equivalent to a personal identification number in order to serve on the board. Web pages of digital businesses must observe information requirements such as its legal address, contact information and value-added tax (VAT) number (if applicable).

CONTRACTING ON THE INTERNET

Contract formation

6 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?

There are no special 'internet requirements' as to the form of the contract or acceptance of contracts in order to be valid. Thus, an electronic contract concluded by 'click wrap' will in principle be enforceable. However, use of an electronic form could be subject to challenges concerning the acceptance of the contract and whether the conditions were presented to the accepting party if, for example, the terms of the contract are unusual or biased.

Applicable laws

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

The e-Commerce Act governs certain aspects of contracting on the internet. The customer must be informed about all technical steps used to conclude the contract, including whether:

- the concluded contract will be filed by the seller and whether it will be accessible at a later stage;
- the technical means of identifying and correcting input errors before the placing of the order; and
- the languages offered for the conclusion of the contract.

Further, the service provider has to acknowledge receipt of an order without undue delay and by electronic means, and make available to the recipient of the service appropriate, effective and accessible technical means allowing him or her to identify and correct input errors before placing the order. Some of the provisions of the e-Commerce Act are mandatory in business-to-consumer relations.

Electronic signatures

8 How does the law recognise or define digital or e-signatures?

Norway has implemented the eIDAS Regulation, which enables the use of electronic identification means and trust services, ie, e-signatures, electronic seals, time stamping, registered electronic delivery and website authentication. An e-signature is defined as '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'. In accordance with the eIDAS Regulation, there is a distinction between 'electronic signatures' and 'advanced electronic signatures'. The rules state that all trust service providers, both qualified and non-qualified, shall take technical and organisational steps to address the security risks associated with the services they provide.

Further, the providers shall notify the Norwegian Communications Authority of security incidents or violations of integrity that to a significant extent affect the trust service.

Data retention

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

A consumer must have the opportunity to save the contract terms when the contract is concluded. There are no general 'internet requirements' imposed on the seller in terms of saving the data for a certain period of time, but it is recommended in case of disputes in the future. Entities covered by the Bookkeeping Act must keep certain accounting records for up to five years from the end of the financial year to which the records relate. The Bookkeeping Act distinguishes between primary and secondary documentation. Primary documentation must generally be retained for five years. The requirement for the retention of secondary documentation is three and a half years. Some sectors and transactions are subject to a 10-year retention period, such as project accounts in the construction and engineering sector and customer and supplier specifications in banks. Other retention requirements may also apply for special transaction types specifically regulated by law.

Breach

10 Are any special remedies available for the breach of electronic contracts?

There are no special remedies available for breach of electronic contracts. There is, however, a complaints board set up for electronic communication, lowering the threshold for consumers to utilise and enforce remedies available on general law.

SECURITY

Security measures

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

The Electronic Communications Act requires any party that provides a public electronic communications service to implement appropriate measures to ensure that the data processed is protected. Network providers shall maintain such standards as are necessary to maintain protection within the network. Consequently, encryption is mandatory if and insofar as it is necessary to protect communication and data within the network. These measures will ensure a level of security that, taking into account the available technology and costs of implementation of the measures, is adapted to the risk of infringement of privacy.

The security of internet transactions as such is primarily handled by statutory requirements to providers of electronic private keys through the Electronic Signatures Act. However, a general duty of care applies and the company or internet service provider (ISP) may become liable if this duty is not fulfilled. Further, processing of personal data is subject to security regulations as stated in the Personal Data Act.

Government intervention and certification authorities

12 | 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?

According to section 19a of the Criminal Procedure Act, the police may instruct anyone who is dealing with a 'computer system' to provide the necessary information to allow access to the system or to open it using biometric authentication. If someone refuses to comply with an order of biometric authentication, the police can enforce the authentication with force.

Pursuant to the eIDAS Regulation, Norway is required to ensure interoperability and security of electronic identification schemes. The Norwegian Communication Authority has been designated as the regulator for electronic identification and trust services.

The eIDAS Regulation introduces 'trust services', which can include:

- the formation, validation and verification of e-signatures, e-seals or electronic time stamps;
- the formation, validation and verification of certificates for website authentication; or
- preservation of e-signatures, seals or certificates. The providers of such services are classified as qualified or non-qualified.

According to the eIDAS Regulation, a trust service provider will be liable for intentional or negligent damages to any natural or legal person if the trust service provider fails to comply with the obligations under the eIDAS Regulation. In the event a trust service provider has informed its customers in advance of the limitations on the use of its service, the eIDAS Regulation states that the trust service provider will not be liable for damages arising from the use of services exceeding the indicated limitations.

Electronic payments

13 | Are there any rules, restrictions or other relevant considerations regarding the use of electronic payment systems in your jurisdiction?

Electronic payment systems may be offered by banks, eMoney businesses, payment providers and financial institutions with a license from Norwegian authorities. Payment systems are regulated through:

- the Financial Undertakings Act;
- the Financial Contracts Act;
- the Payment Systems Act; and
- the Regulation on Payment Service Systems.

Electronic payment services may also be offered in Norway by foreign institutions based on licensing regulations that apply in their respective country of origin. It is a prerequisite that the home country has reported cross-border activities to Norwegian authorities. Norwegian subsidiaries of foreign institutions must comply with Norwegian regulations. Foreign institutions must comply with Norwegian regulations, which are mainly based on common EU/EEA legislation.

Payment services systems must be designed and operated in order to safeguard the security and efficiency of payment and the rational and coordinated execution of payment services. Changes or new systems for payment services must be reported to the Financial Supervisory Authority.

The Central Bank of Norway and the Financial Supervisory Authority are, according to the Payment Systems Act, the supervisory authorities for the Norwegian payment systems and for the payment services and exercise this work through close cooperation.

Use of electronic payment systems is widespread in Norway, with the bank joint venture Vipps as the market leader. This solution includes customer-to-customer payments without charge.

14 | Are there any rules or restrictions on the use of digital currencies?

Issuance of eMoney is regulated in particular to ensure effective right of users to exchange the digital currencies back to hard currency. Use of digital currencies is not regulated. Lower level courts have accepted the right of banks to deny customer relationship with a bitcoin exchange provider. The Financial Supervisory Authority has, however, recently issued a licence to the exchange provider, which in May 2019, was finally able to secure access to a bank account. The matter illustrates the current struggles financial actors have grappling with digital currencies.

DOMAIN NAMES

Registration procedures

15 | 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?

A .no domain name must be registered through a domain registrar (private providers of domain names certified by the government), which will handle correspondence with UNINETT Norid, the government's administrator of .no domain names, on behalf of the applicant. Norid will decide whether the application will be granted and the decision may be appealed. Legal entities applying for domain names must be registered in the Norwegian Register of Business Enterprises and have a Norwegian postal address, and actual business activity must be documented in accordance with what is registered. Private individuals may also register up to five .no domain names if they are over 18 years of age, are registered in the Norwegian National Registry with a Norwegian social security number and have a Norwegian postal address. The rules for the .no domain name do not include any procedures for foreign companies and private individuals registering .no domain names, although it may be technically possible to use a Norwegian intermediary to register a domain name.

Rights

16 | Do domain names confer any additional rights beyond the rights that naturally vest in the domain name?

The registration of a domain name does not change the status of any other rights per se, but may be invoked as a factual circumstance in proving the right of a trademark being established by use.

Trademark ownership

17 | Will ownership of a trademark assist in challenging a 'pirate' registration of a similar domain name?

Trademark infringement is one of the most common grounds for challenging a domain name registration. The trademark owner may demand that an infringing domain name is deleted from the domain name register or transferred to the trademark owner. Cases concerning trademark infringing domain names may be brought before the Norwegian Alternative Dispute Resolution Committee or the ordinary courts of Norway.

Dispute resolution

18 | How are domain name disputes resolved in your jurisdiction?

Domain name disputes are typically resolved through the Norwegian Alternative Dispute Resolution (ADR) Committee. Claimants may file a complaint against Norwegian domain names (country code .no) with the ADR Committee within three years from the registration date of the domain name. The filing cost for a complaint is currently NKr5,750 (€590). Cases before the ADR Committee are resolved through written proceedings, although a party may request oral mediation. Upon receiving a complaint, the ADR Committee will forward the complaint to the respondent with a deadline to submit a reply. If the respondent does not submit a reply within the deadline, the ADR Committee will decide the case based on the complainant's presentation of the facts. If the complainant prevails, the domain name will either be deleted or transferred to the complainant. The ADR Committee usually renders a decision within three months of receiving a complaint. A decision from the ADR Committee may be appealed before the ordinary courts of Norway. A complainant may also bring the case directly before the ordinary courts without filing a complaint before the ADR Committee.

ADVERTISING

Regulation

19 | What rules govern advertising on the internet?

On a general level, the Marketing Control Act and the Electronic Commerce Act govern internet advertising.

The basic requirement is that all marketing be honest and correct and in accordance with fair marketing practices, as further developed in case law over the years. Misleading advertising, passing off, comparative advertising, combination offers and so on are prohibited or strictly regulated. Norway has implemented the Unfair Commercial Practices Directive, including Annex I which states that certain commercial practices shall always be considered unfair and thus illegal. The use of email, fax or an automated phone system (automatic dialler) for advertising without the prior consent of the recipient is also in general prohibited.

Definition

20 | How is online advertising defined? Could online editorial content be caught by the rules governing advertising?

Online advertising is not defined by law and online editorial content is not explicitly governed by law. However, rules concerning advertising in the Marketing Control Act generally apply to all advertising, including advertising online. Online editorial content which, based on an assessment of the facts and circumstances, is deemed to constitute advertising will be subject to the requirements in the Marketing Control Act. Further, the Marketing Control Act specifically states that 'marketing shall be designed and presented so that it clearly appears as marketing'. Similarly, Norwegian media ethics rules require that the press distinguish between editorial content and advertising. Consequently, the manufacturer of editorial content is responsible for ensuring that advertising does not appear to be editorial content.

Misleading advertising

21 | Are there rules against misleading online advertising?

The general prohibition against misleading marketing also applies to misleading online advertising and to all industries. This entails, inter alia, that all marketing be honest, fair and not misleading, including that marketing not omit information that, depending on the circumstances, is significant. All advertising claims must be substantiated, particularly comparative advertising. Advertisers are required to keep on record sufficient information to substantiate any advertising claims made, such as in-depth comparative test results and comparative price data.

Restrictions

22 | Are there any products or services that may not be advertised on the internet?

There are no prohibitions against advertising specifically on the internet, but general advertising bans prohibit advertising certain products and services, such as alcohol, tobacco and gambling, and such bans typically also apply to internet advertising.

Hosting liability

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

The act of creating content is not in itself illegal; it is the actual act of advertising and of using the content, that is prohibited. However, depending on the circumstances, content providers, ISPs and other parties may be liable for contributing to the illegal advertising. A technical contribution is typically not sufficient to incur liability, whereas actively creating content for and contributing to planning of illegal advertising may arguably be sufficient to incur liability.

The e-Commerce Act, implementing the e-Commerce Directive, limits liability for content for 'mere conduit' services, as well as caching and hosting content of which the ISP does not initiate transmission, provided that the ISP does not select the recipient of the transmission and does not select or modify the information contained in the transmission. The ISP's exemption from liability in connection to hosting of content on behalf of the service recipients is conditional upon the ISP not having actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or on the service provider, upon obtaining such knowledge, acting expeditiously to remove or to disable access to the information.

FINANCIAL SERVICES

Regulation

24 | 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?

In addition to the Marketing Act, the Financial Contracts Act regulates financial services products in general, but there is no specific regulation of financial services products sold via the internet. Sales of financial services products are subject to a vast range of provisions, with complex and diverse regulation of different fields, compliance with which should be confirmed by local counsel. The advertising and selling of financial services is monitored by the Norwegian Consumer Authority and the Financial Supervisory Authority of Norway. Both institutions handle requests and complaints from consumers and dispatch directions to firms that offer the services in question.

DEFAMATION

ISP liability

25 | Are ISPs liable for content displayed on their sites? How can ISPs limit or exclude liability?

It is arguable that an ISP should be considered as a publisher of the website. However, in most cases, the ISP is only a technical contributor with no involvement in deciding what content is displayed on the website. From this point of view, the ISP is only liable insofar as it contributes to deciding which content is displayed or has clear knowledge of illegal content being displayed on its sites.

The e-Commerce Act, implementing the e-Commerce Directive, limits liability for content for 'mere conduit' services, as well as caching and hosting content of which the ISP does not initiate transmission, provided that the ISP does not select the recipient of the transmission and that the ISP does not select or modify the information contained in the transmission. The ISP's exemption from liability in connection to the hosting of content on behalf of the service recipients is conditional upon the ISP not having actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or on the service provider, upon obtaining such knowledge, acting expeditiously to remove or to disable access to the information.

Pursuant to the Copyright Act, a content owner may submit a motion to the courts for an order imposing ISPs to take measures preventing access to websites where material that is obviously infringing its copyright is made available to a large extent. This has resulted in courts issuing orders to certain ISPs to use Internet Protocol (IP) or Domain Name System (DNS) blocking to prevent access to certain domain names relating to The Pirate Bay and other file-sharing services. However, the measures used so far have proven to be relatively easy to circumvent and it is possible that the courts may be convinced to issue orders for stricter measures in the future.

Shutdown and takedown

26 | Can an ISP shut down a web page containing defamatory material without court authorisation?

No, an ISP does not normally have such authority unless it is stated in the contract or grounds for termination of contract are evident.

INTELLECTUAL PROPERTY

Third-party links, content and licences

27 | Can a website owner link to third-party websites without permission?

Links to third-party websites without the owner's permission are not illegal per se. However, general rules on protection of fair business practices and IP rights also apply to the use of links to websites. For instance, a metasearch of third-party databases has been deemed illegal by Norwegian courts owing to breach of fair business practices. 'Referring links', by which the user clearly leaves the first site and is transferred to the third-party site, will generally not require third-party permission. Use of 'deep linking', where third-party content is accessed without moving the user from the current website, and 'frame links', where the browser window is partitioned into different frames in which material from several websites can be presented simultaneously, increase the risk of IP infringement. Further, linking to IP infringing material stored on third-party websites may itself constitute IP infringement by the website owner, depending on the circumstances.

28 | 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?

Consent from the content owner is generally required for use by other parties. Relevant legislation includes the Marketing Control Act, which prohibits acts contrary to fair marketing practices; and IP legislation such as the Copyright Act, which grants the copyright holder the exclusive right, inter alia, to produce copies of the copyrighted material, and the Trademark Act, which grants the trademark holder the exclusive right to use the trademark. Exceptions to this exclusivity apply, such as the expiry of copyright, exhaustion, private non-commercial use and legitimate quotes.

Criminal and civil sanctions are applicable, although civil sanctions such as temporary injunctions and damages are by far the typical remedy. Regulatory sanctions are generally not applicable.

29 | Can a website owner exploit the software used for a website by licensing the software to third parties?

The website owner may only license software to third parties if the website owner is also the owner of the software in question, or if such right of licensing has been granted by the owner of the software. There is no statutory right of sub-licensing under Norwegian law.

30 | Are any liabilities incurred by links to third-party websites?

If the third-party website includes illegal content, linking to such websites or content may lead to liability for contributory distribution of the illegal content. Further, the owner of the linking website may be liable for any consequences that use of the link will incur on users of the link. In addition, exploitation of efforts, goodwill, creativeness or inventions of others by links to third-party websites may incur liabilities due to violation of IP rights or fair business practices.

Video content

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

Online video content is in principle regulated in the same way as TV content. The Act on Broadcasting and Audiovisual Media Services, which implements the Audiovisual Media Services Directive, applies to both online video content and TV content.

IP rights enforcement and remedies

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

Dawn raids and freezing injunctions are subject to the authority of the courts. Further, IP infringements are generally not subject to public prosecution unless initiated by an IP owner. Dawn raids and freezing injunctions are therefore generally only carried out as a result of a motion from the IP owner, and in any case require a decision from the courts granting such actions.

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

Civil remedies for IP owners include damages, recall, transfer or destruction of material covered by IP rights, search orders, freezing injunctions and orders to prevent access to websites providing access to copyright infringing material.

DATA PROTECTION AND PRIVACY

Definition of 'personal data'

34 | How does the law in your jurisdiction define 'personal data'?

Norway has implemented the General Data Protection Regulation (EU) No. 2016/679 (GDPR) in its entirety, with a few additional regulations, pertaining to, for example, access to employees' email accounts and camera surveillance. This entails that Norway's regulations relating to data protection and privacy is very similar to the regulation in the European Union.

The definition of personal data follows from article 4 of the GDPR, in that personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive data, or special category according to the GDPR, is defined as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. The processing of such data is prohibited unless certain exceptions apply. This is the case, for instance, if the individual has consented or the processing is necessary:

- for the purposes of carrying out the obligations of the controller or of the data subject in the field of employment and social security and social protection law;
- to protect vital interests;
- for the purposes of preventive or occupational medicine, public health, archiving purposes in the public interest, scientific, historical research purposes or statistical purposes.

If data is made completely anonymous, the GDPR will not apply to the processing of that data. To satisfy the requirement of anonymisation in this regard, it has to be impossible to identify a person in the data. For instance, the existence of a key that will 'unlock' the anonymisation will result in the data being considered not anonymous. Pseudonymisation is under no circumstance considered anonymisation of data in this respect.

Registration requirements

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

There is no registration requirement in order to process personal data. Certain companies will have to appoint a data protection officer (DPO). This will be the case for publicly owned companies and companies that systematically monitor individuals on a large scale, or where large-scale processing of sensitive data is part of the company's core activities. Direct marketing companies, ISPs and mobile phone operators will typically have to appoint a DPO.

Cross-border issues

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

The GDPR applies to entities that processes personal data about EU and Norwegian citizens alike. At the same time, it also applies to Norwegian and European companies. A foreign national will enjoy the protection of the GDPR when his or her personal data is processed by a Norwegian or European company.

As a main rule, personal data may only be transferred to countries that ensure an adequate level of protection of the data. Countries that have implemented the GDPR meet this requirement. Transfers to countries outside of the European Union, 'third countries', require the use of the EU standard contract or binding corporate rules. Transfers to the United States require the same, unless the entity in question is certified under the Privacy Shield. Individuals must be informed, through a privacy policy or similar, about their data being transferred to third countries.

Customer consent

37 | 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 requires legal grounds. These may be consent, legitimate interests (based on an assessment of interests weighing the interest of the processor against the privacy interest of the individual), and contractual or legal obligations.

According to the Marketing Control Act, explicit consent (opt-in) is required for direct marketing using email or short message service (SMS). Each marketing email or SMS must also include an opt-out mechanism. The most common mechanism is an unticked tick-box containing a short explanation of the reason why the information is collected with a link to the full privacy policy.

Sale of data to third parties

38 | 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?

A party may sell, transfer or license out personal data and the liability will differ based on the contract between the parties. However, if the data subjects were not informed about the potential selling of their data when the data was collected, or the proper legal grounds were not secured when the data was collected, the recipient of the data might not have the necessary legal grounds to process that data. Thus, for a transfer or similar to succeed, the seller should guarantee that the personal data in question was collected in a legal manner.

Customer profiling

39 | 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?

Cookies can be used based on implicit consent. Assuming that the website in question has a detailed cookie policy and a cookie notification pop-up footer, implicit consent is considered obtained when the data subject visits the website and has not blocked cookies by changing the settings in his or her web browser.

Information about cookies should include the name of the cookie, what data the cookie collects, for what purposes and how long the data is stored for. The regulatory landscape for cookies may change once the EU e-Privacy Regulation is implemented.

Data breach and cybersecurity

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

No, there are no data breach notification regulations specific to e-commerce.

The rules regarding breach notification follow from articles 33 and 34 of the GDPR. Accordingly, the data controller shall, without undue delay, and no later than 72 hours after becoming aware of the breach, notify the Norwegian Data Protection Authority unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller shall communicate the personal data breach to the data subject without undue delay.

41 | What precautionary measures should be taken to avoid data breaches and ensure cybersecurity?

Companies are encouraged to implement both organisational and technical precautionary measures to avoid data breaches and ensure cybersecurity. The Norwegian Data Protection Authority has issued detailed guidelines regarding recommended technical measures, eg, encryption, passwords, strong authentication, security architecture, anonymisation and risk assessments. Recent cases show that non-compliance with the requirements can be subject to sanctions according to GDPR.

Insurance

42 | Is cybersecurity insurance available and commonly purchased?

Yes, cybersecurity insurance is available on the Norwegian market; however, it remains uncommon.

Right to be forgotten

43 | Does your jurisdiction recognise or regulate the 'right to be forgotten'?

Yes, according to article 17 of the GDPR, the data subject shall have the right to have personal data erased if the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, the data subject withdraws his or her consent, the data subject objects to the processing, the personal data has been unlawfully processed or the personal data has to be erased to comply with a legal obligation.

Email marketing

44 | What regulations and guidance are there for email and other distance marketing?

Section 15 of the Norwegian Marketing Control Act provides that direct marketing by the means of email or SMS requires explicit consent (eg, by an unticked tick-box). Exceptions apply to emails directed to companies; however, only email addresses such as post@company.com are included in this exception. Personal work email addresses are not included. An exception also applies for existing customers. There is no specific rule defining exactly when a customer falls within this exception; it must be decided on a case-by-case basis depending on the customer's transaction history. Unsolicited marketing by phone is allowed, provided that calls are not made to anyone in the do-not-call registry managed by the Norwegian Register of Business Enterprises.

Consumer rights

45 | 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?

All Norwegian citizens, as well as all foreign individuals that have their personal data processed by a Norwegian company, have rights according to the GDPR. These rights include, but are not limited to:

- the right to receive information about the processing of their data;
- the right to be forgotten;
- the right to receive a copy of the personal data processed;
- the right to have data corrected or deleted;
- the right to data portability; and
- the right to object to the processing of their data.

Individuals also have the right to complain to the Norwegian Data Protection Authority.

TAXATION

Online sales

46 | Is the sale of online products subject to taxation?

In principle, there is no difference between online product sales and sales through traditional channels such as brick and mortar stores; both are subject to taxation.

Foreign businesses supplying electronic services (e-services) to Norwegian consumers are liable to collect and pay 25 per cent VAT to the tax authorities. The definition of e-services is based on the EU VAT Directive (2206/112/EU) and the EU VAT Regulation (article 7 of the Council Implementing Regulation (EU) No. 282/2011 of 15 March 2011).

The foreign supplier may use the simplified VOES scheme to report and pay VAT. The Norwegian VOES scheme is an equivalent to the EU VAT Mini One-Stop Shop scheme. The VOES scheme is an alternative to ordinary VAT registration in Norway.

Foreign businesses supplying e-services to Norwegian businesses and public enterprises are to be accounted for by the business receiving the services under the reverse-charge mechanism.

Server placement

47 | 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?

Exactly where a server is placed is not relevant for determining tax liability per se. The threshold for becoming subject to corporate tax is rather low. The starting point is that any foreign enterprise will become subject to Norwegian corporate tax if it conducts business activities within Norway or if it hires out employees to work in Norway. Thus, an assessment of tax liability must be made specifically for each foreign enterprise.

Company registration

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

VAT is a general tax on the domestic consumption of goods and services. Businesses supplying goods and services in Norway must register in the VAT register when their supplies or withdrawals of such goods and services exceed NKr50,000 (approximately €5,300) during a 12-month period. For tax purposes, internet sales are in principle no different from traditional retail outlet sales.

Returns

49 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 principle that commercial and financial relations between associated enterprises should take place on the same terms as if the transaction had taken place between independent enterprises under comparable conditions and circumstances is followed by an obligation to document the price determination at the request of the tax authorities.

Transactions of goods to or from Norway are treated as import and export supplies, with the associated customs formalities. Norwegian VAT-registered businesses calculate VAT on imports of goods and report this on the VAT return. There is no VAT payable upon importation provided that the goods are for use in the VAT registered business. For non-VAT-registered businesses and consumers, the import VAT is payable on the time of importation to Norway. The VAT is calculated on the transactional value of the goods.

GAMBLING

Legality

50 Is it permissible to operate an online betting or gaming business from the jurisdiction?

Betting and gambling businesses can only be operated in Norway under a Norwegian gambling licence from the government. Gambling licences are issued by the Norwegian Gaming Authority. However, the market is currently restricted to selected companies in which the government is a majority owner, such as Norsk Tipping and Norsk Rikstoto and certain charity organisations, the sum of which is commonly referred to as the Norwegian gambling monopoly.

Despite the ban on marketing, offering and providing access to unlicensed gambling products and services, Norwegian private individuals transfer vast amounts of money each year to online gambling websites operated from abroad. In 2010, the Norwegian authorities enacted a prohibition against processing payments to and from unlicensed gambling, for the purpose of preventing such gambling. The prohibition has proven to be ineffective in practice, owing to widespread access to payment processing intermediaries that Norwegian banks are not prevented from processing payments to and from.

The European Gaming and Betting Association has filed a complaint against the Norwegian gambling monopoly to the European Free Trade Association Surveillance Authority, a case that is currently pending. The Norwegian parliament passed a resolution in 2018 instructing the government to prepare legislation aimed at further preventing access to online gambling websites operated from abroad, including authorising the Norwegian Gaming Authority to order ISPs to prevent access to such websites through the use of domain name system DNS blocking. Such legislation has not yet been enacted.

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

The use of online casinos and betting websites is not prohibited by law (in contrast to offering such services). There is no verification required by law for users of online casinos or betting websites, simply because offering such services is illegal and thus not further regulated. Use of foreign-based websites for various gambling activities is not uncommon in Norway.

OUTSOURCING

Key legal and tax issues

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

There are no specific laws, including tax laws pertaining specifically to outsourcing. Consequently, each outsourcing arrangement will be specific to its own particular facts and will raise different legal issues. However, rights of employees can easily be triggered. Intragroup services are transactions between related parties, thus, transfer pricing regulations apply. In case of rendering or receiving intragroup services, number of factors, ie, that the pricing policy of the services is in accordance with the arm's length principle, must be considered in order to prevent possible tax risks. Another key tax issue, where the service provider and the principal or customer are not resident in the same jurisdiction, is whether the service provider constitutes a permanent establishment of the principal or customer in the relevant jurisdiction.

Employee rights

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

An employer that regularly employs at least 50 employees shall provide information concerning issues of importance for the employees' working conditions and discuss such issues with the employee representatives. The same applies where the employer is bound by collective bargaining agreements. The obligations regarding information and consultation include information concerning the current and expected development of the undertaking's activities and economic situation, information and consultation concerning the current and expected workforce situation in the undertaking (ie, cutbacks) and the related measures considered by the employer, and information and consultation concerning decisions that might result in considerable changes in the organisation of work or conditions of employment. Outsourcing will typically be subject to information and consultation with the employee representatives.

The outsourcing of services might be regarded as a transfer of undertaking. According to Chapter 16 of the Working Environment Act, which is derived from two EU Council Directives, the transferor and the transferee must as early as possible provide information concerning the transfer and discuss it with the employee representatives. In particular, information should be given concerning the reason for the transfer, the agreed or proposed date for the transfer, the legal, economic and social implications of the transfer for employees, changes in circumstances relating to collective bargaining agreements, measures planned in relation to the employees, rights of reservation or preference and the time limit for exercising such rights.

Further, the transferor and the transferee should as early as possible inform the affected employees about the transfer and the above-mentioned matters. Collective bargaining agreements may set out additional requirements or regulations with respect to the employers' responsibilities in the event of a transfer of undertaking.

As a result of the transfer, the employment relationships of the employees involved in the transfer will automatically be transferred to the transferee, which will become their new employer. All contractual terms and conditions in force immediately before the transfer will remain in force after the transfer. Specific rules apply with respect to collective bargaining agreements and collective pension schemes. The employees may, however, use the right of reservation, thereby objecting to the transfer to the new employer. As a main rule, such reservation implies that the employment relationship is terminated at the transfer date.

Outsourcing will not always be regarded as a transfer of undertaking. The employment relationships of the affected employees will in these situations remain with the employer. A transfer of undertaking does not in itself give grounds for termination of employment relationships; however, redundancies following a transfer of undertaking may in certain cases give grounds for termination. In a redundancy situation, the employer is obligated to consult with the employee representatives regarding the workforce reductions and with each employee before deciding to give notice of dismissal.

Through the consultation procedures, the employer shall receive all relevant information with respect to which employees that is to be made redundant. If the employer does not consult each employee before it decides to terminate employment and the employee contests the validity, the result may be a judgment that the notice is unwarranted and invalid.

Norwegian legislation has no mandatory redundancy or severance payments to employees. It is mandatory to give dismissed employees their normal salary and other benefits arising from their employment agreement during the period of notice. However, it is quite common to offer severance payments or exit packages to avoid disputes.

All of the rules mentioned above apply to all employees within the jurisdiction. However, and as indicated above, the information and consultation obligation may be different depending on whether collective bargaining agreements apply.

ONLINE PUBLISHING

Content liability

54 When would a website provider be liable for mistakes in information that it provides online? Can it avoid liability? Is it required or advised to post any notices in this regard?

If the website provider is only responsible for providing a technical service, it will typically not be liable for mistakes in information unless such mistakes are due to errors in the technical service, or if the website provider's technical service is wilfully or negligently promoting such mistakes, or otherwise entails that the website provider is complicit in the mistakes. If the website provider is the responsible editor, liability for mistakes will be triggered if third-party statutory rights are violated, such as defamation, invasion of privacy or IP infringements. For issues contributing to a debate of general interest, the Supreme Court has accepted a certain degree of blameworthiness in the media's presentation without imposing liability for mistakes. In recent years, the Supreme Court has rendered several verdicts imposing liability on newspapers for publishing incorrect and otherwise defamatory information, which arguably indicates a stricter liability for publishers' mistakes. The liability is mandatory and cannot be avoided except by agreement with the plaintiff. If a website provider discovers incorrect information, correcting the information and posting notices informing that the incorrect information has been corrected may prevent or limit liability. Depending on the circumstances, notices may be a relevant consideration in the overall assessment of liability or the calculation of damages. However, preemptive notices, for example, a blanket statement that the information provided cannot be relied upon, or a general limitation waiver, are often ineffective at preventing liability. A website provider that has posted (eg, defamatory information cannot prevent liability through such notices).

Databases

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

Databases are protected as a separate category in the Copyright Act. Using a database or data from a database is not in itself prohibited, but commercial copying or reproduction of data from a database requires permission from the database owner, such as a website provider that includes databases on its site. Infringements of database rights can be pursued through various remedies such as temporary injunctions and claims for damages. Some exceptions apply, such as expiry of copyright, exhaustion, private non-commercial use and legitimate quotes.

SCHJØDT

Jeppe Songe-Møller
jsm@schjodt.no

Kaare M Risung
kmr@schjodt.no

Trond Larsen
trla@schjodt.no

Øivind K Foss
oifo@schjodt.no

Marie Berggren Hagberg
mabe@schjodt.no

Ruseløkkveien 14
PO Box 2444
Solli
0201 Oslo
Norway
Tel: +47 22 01 88 00
www.schjodt.no/en/

DISPUTE RESOLUTION

Venues

56 Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

The Norwegian courts are technology neutral. There are no specialist courts or venues that specifically deal with online/digital issues and disputes.

ADR

57 What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

The Norwegian ADR Committee processes domain name complaints. The ADR Committee handles almost all domain name disputes in Norway. More generally, the parties may agree to resolve such disputes through arbitration, court-assisted mediation, in-court mediation or various industry-specific committees (eg, the Norwegian Financial Services Complaints Board).

UPDATE AND TRENDS

Key developments of the past year

58 Are there any emerging trends or hot topics in e-commerce regulation in the jurisdiction? Is there any pending legislation that is likely to have consequences for e-commerce and internet-related business?

The GDPR is expected to impact e-commerce in terms of continued focus on lawfulness of processing (consent versus necessity of performance of contract versus legitimate interest), incompatible processing (eg, retargeting), profiling and data security. The e-Privacy Regulation will likely clarify the regulatory landscape for cookies.

Norway enacted a new Copyright Act on 15 June 2018, with the purpose of modernising and simplifying existing copyright legislation. The Act does not entail any significant departure from the old Copyright Act, although certain new rules such as a prohibition against unauthorised streaming of copyrighted material have been added.

The Norwegian Government issued a draft act for transposing the NIS Directive into Norwegian law on 21 December 2018. The time limit for comments expired on 22 March 2019. The draft act is currently pending further revision based on the comments received.

The Norwegian foundation Lovdata has published laws and court decisions online since 1981. In 2018, certain private individuals re-published a large number of court decisions originally published by Lovdata on the domain name rettsdata.no. A case is now ongoing before the Norwegian courts to decide whether such re-publishing constitutes an infringement of Lovdata's copyright or database rights. The Court of Appeals concluded with infringement. An appeal has been filed and accepted by the Supreme Court, which is expected to hear the case during autumn 2019.

A decision on whether to incorporate the DSM Directive is currently being considered by the European Free Trade Association (EFTA). The Norwegian Ministry of Justice and Public Security has previously published its assessment that the DSM Directive is relevant to EFTA and did not indicate any necessary amendments for incorporation into Norwegian law.

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
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 Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

ISBN 978-1-83862-138-4