lead to disputes, and there will be limits on what smart contracts can do. Lawyers, regulators and the court systems would need to become familiar with smart contracts.

Recordkeeping requirements and evidentiary rules would need to be adapted to enable access to underlying data by courts and other authorities.

▷ **Privacy and Security:**

The technology relies on an assumption that it is very secure because records would be almost impossible to decrypt. However, with the continued development of quantum computing, this may not always be the case. There are other security concerns, for example, that it could be possible to trace or deduce a party's identity from transactions or through access to a party that has permission to decrypt the data. In theory, at least, a ledger might also be "captured" if someone were able to control the majority of participating computers.

▷ **Competition/Anti-Trust:**

If private distributed ledgers are created that are equivalent to consortia, there could be arguments of monopolistic or cartel activity. Also, there could be a risk that algorithms are set up in a manner which produces anti-competitive results that are secret or not readily detectible.

▷ **Decentralised Organisations:**

There are various issues that would need to be considered in terms of liability and accountability as existing legal systems are primarily designed to assign responsibilities and liabilities to persons (human or legal) rather than to a mechanism such as a distributed ledger that involves automated contracts. Lawmakers may need to consider how to adapt the existing law related to liability in the context of unincorporated associations to deal with the operation of distributed ledgers, which may be particularly challenging to the extent that these are likely to operate across borders.

V. Conclusion

It's clear that distributed ledger technology has significant potential to transform a variety of sectors and scenarios, and an increasing number of organisations are considering how this technology could be used in their own businesses. However, the technology is not a panacea, despite what some of the overblown headlines might suggest. While certain transactions may benefit from decentralisation, it's likely that many others will still need to be handled via an intermediary and central database. Proper cost/benefit and risk analysis will be vital to ensure that this technology does not overpromise and under-deliver.

Michaela Weigl

The EU General Data Protection Regulation's Impact on Website Operators and eCommerce

Essential changes for Privacy Statements, Consent, Direct Marketing and Cookies

On 25 May 2016, the EU General Data Protection Regulation ("GDPR") entered into force within the European Union. When the GDPR becomes applicable on 25 May 2018 (Art. 99 (2) GDPR), it will replace the Data Protection Directive 95/46/EC "over night" (unless transition periods will be implemented, e.g. on a national level). The GDPR will, inter alia, impact a company's Internet presence, including webshops. Therefore, companies operating a website and/or a webshop should consider rather sooner than later how the GDPR will impact their website documentation and data processing practices on their websites in order to be compliant by 25 May 2018. Given the GDPR's expanded scope this does not only apply to EU based companies that operate a website and/or a webshop, but also to companies outside the EU that, for example, operate a webshop and offer goods or services to customers in the EU, or companies that operate a website and place cookies on their customers' computers in the EU and in doing so monitor the behavior of customers in the EU, Art. 3 (1) and (2) GDPR.

This article focusses on four topics of particular interest for companies that operate a website and/or webshop and the upcoming changes in this regard: (I.) Privacy Statements, (II.) Customer's Consents, (III.) Direct Marketing, and (IV.) Cookies.

I. Privacy Statements

The GDPR[1] retains most of the information obligations, but partly amends and expands them. Companies operating a website and/or a webshop will therefore be required to review and update their website Privacy Statements. In detail:

1. Content

Art. 13 GDPR contains a list with information that must be provided to website users.

▷ Dr. Michaela Weigl, Frankfurt/Main. Further information about the author at p. 128. This article reflects the author's personal opinion and not those of Baker & McKenzie, its clients or others. The article is based on the presentation of the author on 29 June 2016 at the "Expert Committee Internet and eCommerce" of the German Association of Law and Informatics ("Deutsche Gesellschaft für Recht und Informatik").

1 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, available in various languages at: *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.*

a) More Than Mere Contact Details

Companies do not only have to inform about their identity and the contact details, but, where applicable, also about the company's representative (Art. 13 (1) a) GDPR). The latter applies, when a company is located outside the EU (e.g. in the US) and e.g. offers goods to EU citizens because in such case the company is required to designate a representative in the EU.[2]

The term "contact details" is not defined in the GDPR. Recital 23 states "an email address or of other contact details" and therefore implies that an email address is a "contact detail". There are good arguments that "contact details" means the address, arguably also an email address. Additionally, companies must provide the "contact details" of the data protection officer, if any (Art. 13 (1) b) GDPR). In contrast to the information about the company, it is not required to inform about the data protection officer's name, it is rather sufficient to inform about his "contact details". To avoid having to update the Privacy Statement every time the data protection officer changes it should also be sufficient to provide a link to the "contact details" of the data protection officer and/or to provide a generic email address.

b) Legal Basis For the Processing

In addition to the purposes of the processing for which the personal data are intended, companies will furthermore be required to name the legal basis for the processing (Art. 13 (1) c) GDPR). For website and webshop operators this will in most cases be contract performance (Art. 6 (1) b) GDPR), compliance with a legal obligation (Art. 6 (1) c) GDPR), legitimate interests (Art. 6 (1) f) GDPR) and/or consent (Art. 6 (1) a) GDPR), depending on the concrete data and purpose of the collection/processing. To the extent the data processing is based on national law (e.g. if the legal basis stems from a national implementation of the ePrivacy Directive 2002/58/EC) website operators will also have to name the national law. This new requirement will impose some challenges, in particular for website operators that intend to have uniform Privacy Statements in various EU Member States.[3]

Another requirement that also leads to more drafting effort is the requirement to inform about the legitimate interests if the processing is based on the balancing of interests justification - Art. 6 (1) f) GDPR (Art. 13 (1) d) GDPR). In such case, website operators are required to state their legitimate interests, e.g. for using a service provider outside the EU to provide hosting services.

Website/webshop operators must also inform about whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the user is obliged to provide the personal data and of the possible consequences of failure to provide such data (Art. 13 (2) e) GDPR). This requirement might also impose some difficulties when drafting uniform Privacy Statements for more than one EU jurisdiction because the provision of personal data might be statutory in one EU Member State but voluntary in another EU Member State. In case of the existence of automated decision making, including profiling, it is required to inform about that fact and provide meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the customer (Art. 13 (2) f) GDPR).[4]

c) Recipients of the Personal Data

As under the Directive 95/46/EC website and webshop operators must inform about the recipients or categories of recipients of the personal data, if any (Art. 13 (1) e) GDPR). If the data is intended to be transferred to a third country, companies that operate a website or webshop must additionally inform about that fact and the existence or absence of an adequacy decision, or in the case the transfer is based e.g. on EU Model Clauses or Binding Corporate Rules, provide a reference to such documents in the Privacy Statement and the means by which to obtain a copy of them or where they have been made available (Art. 13 (1) f) GDPR). As a consequence that means that website and webshop operators must make available, e.g. their (intra-group) data processing agreements to customers and users, at least upon request.[5]

d) Data Storage Period

Another new information obligation is the requirement to inform about the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period (Art. 13 (2) a) GDPR). Since retention periods depend on various factors (e.g. relevance from a tax law perspective), companies will likely have to inform about the criteria used to determine the retention period (e.g. data relating to the purchase of a product will be deleted after the expiry of the statutory limitation period).

e) Rights of the Data Subject

As under the Directive 95/46/EC, website and webshop operators must also inform about the user's rights, i.e. about the right to access and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability (Art. 13 (2) b) GDPR). Since the wording of the GDPR does not require more, it should be sufficient to just inform about these rights without providing any further details (e.g. prerequisites when these rights exist).

Additionally, companies must inform about the right to lodge a complaint with a supervisory authority (Art. 13 (2) d) GDPR). If the processing is based on consent website and webshop operators must also inform about the existence of the right to withdraw consent any time

2 See Art. 27 GDPR. The representative shall in particular be mandated to be contacted by the data protection authorities and customers on issues regarding the processing.

3 The legal bases might vary among the Member state. The requirement also constitutes issues regarding the timing of updating the Privacy Statement or regarding the correct wording in the Privacy Statement: Since national data protection laws still apply until May 25, 2018 the legal bases of the GDPR are true only from that date. It is also doubtful whether inserting (a number of) legal bases in a Privacy Statement for consumers is compatible with the requirement to provide the information in a transparent, intelligible form, using clear and plain language (see Art. 12 (1) GDPR).

4 Please see below (IV. 2. b) and 3.) in more detail.

5 See also *Härting*, Datenschutzgrundverordnung, 2016, recital 59.

without affecting the lawfulness of processing based on consent before its withdrawal (Art. 13 (2) c) GDPR).

f) Data Categories and Source of Personal Data

If personal data has not been obtained from the data subject, website and webshop operators must additionally inform about the categories of personal data concerned (Art. 14 (1) (d) GDPR) and from which source the personal data originate, and if applicable, whether it came from publicly available sources (Art. 14 (2) f) GDPR).

Further information requirements might apply, e.g. if national law imposes them.[6]

2. Formal Requirement: Transparency

Art. 12 (1) GDPR requires that the above listed information must be provided in a concise, transparent, intelligible and easily accessible form using clear and plain language.

It remains to be seen how "clear and plain language" will be interpreted. The information should be easily accessible if provided via a link on the website.[7] The information may also be provided in combination with standardized icons, which are to be adopted by the EU Commission in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing.

3. Timing

As before, the information shall be given at the time when personal data are obtained (Art. 13 (1) GDPR). However, if the data are not obtained from the user/customer, the information must be provided within a reasonable period after obtaining the personal data, but at the latest within one month, depending on the specific circumstances (Art. 14 (3) GDPR).

4. Possible Sanctions

A violation of the information obligations may be sanctioned with administrative fines up to EUR 20 Mio. or up to 4% of the total worldwide annual turnover (Art. 83 (5) b) GDPR).

II. Consent

Consent remains as legal justification for the processing of personal data. The GDPR partly stipulates what has been the law or practice of data protection authorities already for many years, however it also sets out new stricter requirements. It is, however, not necessary for the user/customer to give his consent again if the manner in which the consent has been given is in line with the conditions of the GDPR (recital 171 GDPR).

1. Requirements

Consent must be freely given, specific, informed and unambiguous (Art. 4 No. 11 GDPR):

a) "Freely Given" Consent

Freely given means that the customer has a genuine or free choice or is able to refuse or withdraw consent without detriment (recital 42 GDPR). Consent will not be deemed "freely given" if the performance of a contract is dependent on consent despite such consent not being necessary for such performance (Art. 7 (4) and recital 43 GDPR). This could, for example, be the case, if the participation in a sweepstake or the purchase of goods depends on the customer's consent to the provision of personal data for marketing purposes.[8] Furthermore, consent should not provide a valid legal ground where there is a "clear imbalance" between the data subject and the controller (recital 43 GDPR). It remains to be seen how the term "clear imbalance" will be interpreted, e.g. as already interpreted by many data protection authorities in employment relationships, or if such "clear imbalance" could also be given if a consumer concludes a contract with a company[9]. In the latter case, data processing could barely be based on consent any longer. Since the legislator expressly provides for consent as one processing condition and in most cases the consumer has a choice to provide consent to a company or not, the requirement should be interpreted in a manner that a "clear" imbalance between a company and a consumer only exists in exceptional circumstances. Otherwise, relying on consent would become an unsafe solution for website and webshop operators.

b) "Specific" Consent

The definition of consent further provides that consent must be "specific", i.e. general broad consents will likely be invalid. Also, it will be more difficult to argue that consents covering several purposes are valid. Recital 43 provides that separate consent should be obtained for separate personal data processing operations, if appropriate in the individual case. Therefore, it might be required to provide for more checkboxes in order to provide separate consent, e.g. for marketing, market research and a transfer of the user account. However, if a technology only provides for a uniform handling and therefore consent to all measures or none, separate checkboxes might not be required because they are not appropriate.

c) "Informed" Consent

As before, consent requires the data subject to be "informed", i.e. users and/or customers should be aware at least of the identity of the website/webshop operator and the purposes of the processing for which the personal data are intended (recital 42 GDPR).

d) "Unambiguous" Consent

Consent means an unambiguous indication of the customer's wishes by a statement or a clear affirmative action. In the online environment this includes, for example, ticking a box or choosing technical settings of

6 In certain cases the above listed information obligations do not apply (Art. 13 (4), Art. 14 (5) GDPR).

7 See recital 58 GDPR which explicitly states that the "information could be provided electronically, for example, when addressed to the public, through a website".

8 Please see in this regard also *Gierschmann*, ZD 2016, p. 54. However, it can also be argued that when assessing whether consent is "necessary for the performance of that contract", economic necessities have to be taking into account.

9 Please see in this regard also *Härting*, ITRB 2016, p. 40 and *Gierschmann*, ZD 2016, p. 54.

the browser or another statement or conduct which clearly indicates the customer's acceptance of the proposed processing of his or her personal data (recital 32 GDPR). Users and/or customers must have the right to withdraw their consent any time and be informed about their withdrawal right prior to giving consent (Art. 7 (3) GDPR). The right to withdraw consent any time is another factor that leads to uncertainty for website and webshop operators when relying on consent.

2. Form

The formal requirements for consent are generally less strict than under the German Federal Data Protection Act.[10] Consent can be provided, inter alia, by electronic means (recital 32 GDPR). However, Art. 7 (1) GDPR expressly requires that the controller must be able to demonstrate that the data subject has consented. If consent is pre-formulated by the controller (as is mostly the case on websites) the consent declaration should be provided in an intelligible and easily accessible form, using clear and plain language (recital 42 GDPR). It remains to be seen how strict these requirements will be interpreted. If consent is included in written declarations which also concern other matters, e.g. in terms and conditions, the request for consent must be presented in a manner which is clearly distinguishable from the other matters (Art. 7 (2) GDPR). This could for example be done by using bold letters or by framing the consent wording, e.g. for market research. However, it is not yet clear, how the provision of consent(s) in terms and conditions is compatible with the requirement of providing separate consent.[11]

3. Possible Sanctions

Non-compliance with consent requirements may be sanctioned with administrative fines up to EUR 20 Mio. or up to 4% of the total worldwide annual turnover (Art. 83 (5) a) GDPR).

III. Direct Marketing

Companies operating a website or webshop should also check whether their direct marketing practices comply with existing laws.

1. Legal Basis

Unlike the German Federal Data Protection Act, the GDPR does not provide for a specific legal basis for direct marketing. However, the general "principle of prohibition unless permitted" applies, i.e. processing of personal data for marketing purposes is lawful only if and to the extent that a permission applies.[12] There are good arguments that under the GDPR the use of personal data for marketing purposes can be based on a legal justification without the need for consent:[13]

a) Necessity for Contract Performance

Art. 6 (1) b) GDPR might be applicable as a legal basis because it allows for a processing of personal data if the processing is necessary in order to take steps at the request of the data subject prior to entering into a contract.[14] Marketing usually takes place prior to entering into a contract. Additionally, it could be argued that the provision of personal data is the request to take steps, e.g. the provision of the email address to a website or webshop operator is the request for receiving newsletters and marketing.

b) Legitimate Interests

There are good arguments that Art. 6 (1) f) GDPR constitutes a permission for direct marketing.[15] Art. 6 (1) f) GDPR contains the balancing of interests and states that a processing is lawful if processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. Recital 47 explicitly provides that the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. Marketing/advertisement is also protected by the freedom of goods[16], the Charter of Fundamental Rights of the EU[17], the European Convention of Human Rights[18] as well as e.g. by the German Constitution[19]. Therefore, there are good arguments that website providers or webshop providers may rely on the legal justification in order to use personal data for own direct marketing purposes. Since Art. 6 (1) f) GDPR considers not only the legitimate interests of the controller but also the legitimate interests of a third party, the use of personal data for direct marketing for products and/or services of third parties should also be covered.[20] Recital 47 states that the existence of a legitimate interest requires a careful assessment, including whether a data subject can "reasonably expect" at the time and in the context of the collection of the personal data that processing for that purpose may take place. There are good arguments that customers need to expect that personal data is used also for direct marketing of third party products and/or services. It remains to be seen how "reasonable expectations" - a term reminiscent of U.S. data protection law - will be interpreted, e.g. whether objective or subjective (or both) criteria matter.[21]

10 *Härting*, Datenschutzgrundverordnung, 2016, recital 357.
11 Further requirements regarding consent apply, e.g. in case of sensitive data or if a child is involved.
12 See also *Gola/Schulz* K&R 2015, p. 610.
13 See also *Härting*, Datenschutzgrundverordnung, 2016, recital 480.
14 See also *Gola/Schulz* K&R 2015, p. 610.
15 See also *Gola/Schulz* K&R 2015, p. 611.
16 Court of Justice of the European Union, judgment dated 6 July 1995, File No. C-470/93.
17 Art. 11 Charter on Fundamental Rights, see *Streinz*, EUV/AEUV, 2nd edition 2012, Art. 11 recital 12.
18 Art 10 European Convention of Human Rights, see e.g. European Court of Human Rights, judgment dated 19 February 2015 – file No. 53649/09, NJW 2016, 781 seq.
19 Art. 2 (1), 5, 12, and/or 14 German Constitution might be applicable; German Federal Constitutional Court, decision dated 11 February 1992 – File No. 1 BvR 1531/90, NJW 1992, 2341; German Federal Constitutional Court, judgment dated 12 December 2000 - File No. 1 BvR 1762/95 and 1787/95, NJW 2001, 591; see also *Gola/Schulz* K&R 2015, p. 611.
20 See also *Gola/Schulz* K&R 2015, p. 612 seq. and *Härting*, Datenschutzgrundverordnung, 2016, recital 481.
21 The right to privacy in the United States is conditioned on a "reasonable expectation of privacy" (US Supreme Court, *Katz v. United States*, 389 U.S.?347 (1967), which requires (i) "that a person have exhibited an actual (subjective) expectation of privacy and, (ii) that the expectation be one that society is prepared to recognize as 'reasonable'". See also *Spies*, ZD, 2011, p. 12.

c) Principle of Purpose Limitation

Art. 5 (1) b) GDPR states the principle of purpose limitation, i.e. requires that personal data must be collected for specified, explicit and legitimate interests and not further processed in a manner that is incompatible with those purposes. Therefore, it should be sufficient if the purpose "direct marketing" is determined before the collection of the personal data. If a website or webshop operator wants to use existing contract data, i.e. data that has already been collected for another purpose (e.g. contract conclusion), for "direct marketing" the requirements of Art. 6 (4) GDPR must be complied with.[22] Art. 6 (4) GDPR provides that if the processing for the other purpose is not based on consent, the controller must ascertain that the processing for another purpose is compatible with the purpose for which the personal data are initially collected. When conducting the "compatibility test" the controller must take into consideration, inter alia, any link between the purposes, the context in which the personal data have been collected, in particular the relationship between data subjects and the controller and the possible consequences of the intended further processing. Depending on how strict these criteria will be interpreted, existing customer data might be used for the other purpose direct marketing.

2. Right to Object

If the customer's data is used for direct marketing purposes, the customer has the right to object at any time to processing of personal data concerning him or her for such marketing (Art. 21 (2) GDPR). Customers must be informed about the right to object at the latest at the time of the first communication (Art. 21 (4) GDPR).

3. Possible Sanctions

A missing legal basis and failure to observe or to inform about the direct marketing objection may be sanctioned with administrative fines up to EUR 20 Mio. or up to 4% of the total worldwide annual turnover (Art. 83 (5) a) GDPR).

4. Directive 2002/58/EC and National Unfair Competition Law

If only the GDPR was applicable for the handling of personal data in the direct marketing context, there are good arguments that it would be sufficient to inform the customers/users in the Privacy Statement about the purpose and to inform about the right to object. In contrast Sec. 7 (2) No. 3 of the German Unfair Competition Act states, for example, that sending marketing materials by email requires the customer's prior express consent, i.e. opt-in consent.[23] Sec. 7 (2) German Unfair Competition Act serves the implementation of Art. 13 of Directive 2002/58/EC[24], which states that e.g. the use of "electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent". Since the GDPR only repeals Directive 95/46/EC, Directive 2002/58/EC and its national implementations remain valid.[25] Art. 95 GDPR states that the GDPR does not impose additional obligations in relation to matters subject to Directive 2002/58/EC and recital 173 states that the GDPR applies to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations set out in Directive 2002/58/EC. Therefore, unless an exception applies[26], and depending on the recipient and the medium used, explicit consent for direct marketing might still be required. Recital 173 states that Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with the GDPR.

IV. Cookies

Website and webshop operators should also consider their cookie practice.

1. Personal Data

Under the GDPR it still remains unclear whether for example IP addresses are regarded as personal data and therefore cookies collecting IP addresses must comply with the GDPR.[27] In Art. 4 No. 1 GDPR personal data is defined as any information relating to an identified or identifiable natural person, i.e. a person who can be identified e.g. by reference to an online identifier. In addition, recital 30 states that "natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers" which may leave traces which may be used to identify them. These indicate a rather broad definition of "personal data".[28] On the other hand recital 26 states that to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person, including all objective factors like costs and time required for the identification. It remains to be seen, how data protection authorities will interpret the term.

It is expected that the Court of Justice of the European Union soon provides guidance on whether dynamic IP addresses constitute personal data in case C-582/14, after the Advocate General issued his opinion in May.[29]

22 In more detail see *Gola/Schulz* K&R 2015, p. 613 and *Gierschmann*, ZD 2016, p. 54.

23 Federal Court of Justice Germany, judgment dated 16 July 2008 - file No. VIII ZR 348/06; MMR 2008, pages 731 seq.; Federal Court of Justice Germany, judgment dated 11 November 2009 - file No. VIII ZR 12/08, NJW 2010, pages 864 seq. An English translation of the German Unfair Competition Act is available at *http://www.gesetze-im-internet.de/englisch_uwg/englisch_uwg.html.*

24 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, available at *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML; Ohly/Sosnitza*, UWG, 7th edition 2016, Sec. 7 recital 8; *Köhler/Bornkamm*, UWG, 34th edition 2016, Sec. 7 recital 8.

25 See Art. 95 GDPR, also *Härting*, Datenschutzgrundverordnung, 2016, recital 480.

26 An exception applies if (i) the email address was obtained in connection with the sale of goods or services, (ii) is used for advertising of own similar goods or services, and (iii) the information on the right to object has been given when the address is recorded and each time it is used (see Sec. 7 (3) Unfair Competition Act).

27 *Härting*, ITRB 2016, p. 36 seq.

28 *Härting*, Datenschutzgrundverordnung, 2016, recital 279.

29 See Court of Justice of the European Union, File No. C-582/14. The German Federal Court of Justice referred for a preliminary ruling, inter alia, the question whether Article 2(a) of Directive 95/46/EC must be interpreted as meaning that an Internet Protocol address (IP address) which a service provider stores when his website is accessed, already constitutes personal data for the service provider if a third party (an access provider) has the additional knowledge required in order to identify the data sub-

2. Legal Basis

Depending on the type of cookie various legal bases could apply.

a) Contract Performance and Legitimate Interests

If a cookie is strictly necessary, Art. 6 (1) b) GDPR applies because the cookie (and the processing of personal data) is necessary for the performance of a contract (e.g. shopping basket cookie).

For not strictly necessary cookies there are good arguments that Art. 6 (1) f) GDPR – legitimate interests – applies. If direct marketing purposes may be regarded as carried out for a legitimate interest pursuant to recital 47, one could argue that "indirect marketing purposes" may be regarded as legitimate interest a fortiori. Receiving targeted advertisement or tailored websites seems to be less intrusive than receiving marketing emails. Also, there are good arguments that website visitors can reasonably expect that for example their IP address and the visited websites are used e.g. for targeted advertisement.[30] In the end this will depend on the concrete targeting and tracking measures taken and on the interpretation of "reasonable expectations". However, there are good arguments that consent is not necessary for the placing of cookies.

The key question is whether the requirements set out Directive 2009/136/EC[31] prevail. Directive 2009/136/EC tightened the rules for the use of cookies and similar technologies (web beacons, tracking pixels) in comparison to Directive 2002/58/EC.[32] Under Directive 2002/58/EC an *opt-out approach* (right to object) was sufficient. Directive 2009/136/EC requires an *opt-in approach* (consent), however, it is debated how consent should be obtained[33]. The GDPR does not contain a statement regarding the relationship between the GDPR and Directive 2009/136/EC. One could argue that the GDPR prevails due to the rule of "lex posterior derogat legi priori". However, since Directive 2009/136/EC amends Directive 2002/58/EC, it likely applies in addition to the GDPR. Because Art. 5 (3) of Directive 2009/136/EC contains a reference to Directive 95/46/EC there are good arguments that it now references the GDPR regarding the consent requirements.

It remains to be seen, whether the amended Directive 2002/58/EC will set out the requirements for cookies also in the future or whether it will be amended.[34]

b) Consent

If the use of cookies cannot be based on Art. 6 (1) f) GDPR, consent pursuant to Art. 6 (1) a) GDPR must be obtained. As mentioned above, consent must, inter alia, be unambiguous, i.e. be given by a clear affirmative action. With regard to cookies ticking a box or choosing technical settings of the browser should be feasible ways.[35] However, default manufacturer browser settings might not be sufficient because the customer's acceptance of the proposed processing of his or her personal data is required. Recital 32 states that silence, pre-ticked boxes or inactivity should not constitute consent. On the other hand, recital 32 states that if the request for consent is given by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided. This is a good argument against the practice of asking for consent for the use of cookies, e.g. in pop-up windows or similar, as it can be argued that it disturbs the website browsing.[36]

There are good arguments that explicit consent is not required. Art. 22 GDPR states that the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. This does not apply if the decision is based on the data subject's explicit consent. Profiling is defined in Art. 4 No. 4 GDPR as any form of automated processing of personal data consisting of the use of personal data, e.g. to analyse or predict aspects concerning that natural person's personal preferences, interests, or behavior. Tracking the customer's browsing activities via cookies to analyse their purchasing behavior would be a good example covered by this definition and therefore the decision on what kind of advertisement is provided to the customer/user is based solely on an automated processing. However, the choice of advertisement does not produce any legal effects and there are very good arguments that it does not similarly significantly affect the customer. This applies in particular since the examples in recital 71 include the automatic refusal of an online credit application or e-recruiting practices without any human intervention.

3. Information Obligations: Transparency

Pursuant to Art. 13, 14 GDPR the users should be informed about the use of cookies, e.g. in a Privacy Statement or a Cookie Policy. There are good arguments that website and webshop operators using cookies do not have to inform about the existence of automated decision-making, including profiling, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (Art. 13 (2) (f) GDPR), because the choice of advertisement does not produce any legal effects and there are very good arguments that it does not similarly significantly affect the customer (i.e. the prerequisites of Art. 22 GDPR are not given[37]).

4. Right to Object

Users do not have a universal right to object to the use of cookies/profiling[38], but may only object if profiling is

ject (see Federal Court of Justice CR 2015, 109). In his opinion delivered on 12 May 2016 the Advocate General - Campos Sánchez-Bordona - answered the question in the affirmative (available at *http://curia.europa.eu/juris/document/document.jsf?text=&docid=178241&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1049070*). In this regard please also see *Keppeler*, CR 2016, pages 360 seq.

30 Regarding the term "reasonable expectations" please see above III.1.b).

31 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, available at: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF.*

32 See also *Auer-Reinsdorff/Conrad*, Handbuch IT- und Datenschutzrecht, 2nd edition 2016, Sec. 36 recital 10; *Rauer/Ettig*, ZD 2014, p. 28.

33 Please see *Rauer/Ettig*, ZD 2015, pages 255 seq. Please also see opinions of the Art. 29 Working Party, WP 171, WP 194, WP 208.

34 *Härting*, Datenschutzgrundverordnung, 2016, recital 365.

35 The GDPR expressly allows for consent by choosing technical settings of the browser (recital 32 sentence 2 GDPR).

36 *Härting*, Datenschutzgrundverordnung, 2016, recital 363.

37 Please see above IV. 2.b).

38 The universal right to object only applies for direct marketing, Art. 21 (2) GDPR; in other cases the right to object depends on the legal basis.

based on Art. 6 (1) f) GDPR, i.e. necessary for the purposes of the legitimate interests pursued by the website operator.

5. Possible Sanctions

A missing legal basis and failure to inform may be sanctioned with administrative fines up to EUR 20 Mio. or up to 4% of the total worldwide annual turnover (Art. 83 (5) a) b) GDPR).

V. Conclusion

Companies that operate a website and/or a webshop should prepare for the changes the GDPR requires, update their website Privacy Statements and check whether their consent mechanisms and consent forms comply with the GDPR. With regard to direct marketing and cookies, companies should check whether they are compliant with current law and monitor the European and national legislation.

Uchenna Jerome Orji

A Comparative Review of the ECOWAS Data Protection Act

Regional Data Protection Governance in West Africa measured against European Data Protection Regimes

Following the spread of ICTs and Internet penetration in Africa and growing concerns over the protection of personal data in the information society, some African regional intergovernmental organizations have established legal frameworks on data protection. The Economic Community of West African States (ECOWAS) has adopted a regional Data Protection Act as legal framework to address data protection concerns amongst its member States in West Africa. The ECOWAS Data Protection Act recognizes that advancements in ICTs increases the problem of personal data protection and seeks to address the problem by establishing a harmonized legal framework for data protection in the ECOWAS region. This paper seeks to analyze the ECOWAS Data Protection Act while also comparing it with international data protection regimes such as the EU Data Protection Directive, Council of Europe Data Protection Convention and the EU General Data Protection Regulation. The paper also identifies some data protection governance mechanisms that are missing in the ECOWAS Data Protection Act and proposes the establishment of an institutional data protection governance mechanism within the framework of the ECOWAS framework in order to facilitate the regional harmonization of data protection law and the dissemination of best practices.

The paper is divided into eight sections: The first section briefly examines the concept of data protection (I.). The second section introduces the ECOWAS Data Protection Act and also examines provisions relating to the regulation of data processing activities by National Data Protection Authorities including the authorization of specific data processing activities and regulation of data processing activities in public services (II.). The third section examines the general principles governing the processing of personal data under the Act (III.). The fourth section examines the specific principles governing the processing of "sensitive" personal data (IV.). The fifth section examines the rights of data subjects (V.). The sixth section examines the obligations of data controllers (VI.). The seventh section examines provisions governing trans-border data flows to non-ECOWAS Member States (VII.), while the eighth section examine some data protection governance mechanisms that are absent from the Act (VIII.).

I. The Concept of Data Protection

The Blacks Law Dictionary defines "data protection" as "any method of securing information especially information stored on a computer from being either physically lost or seen by an unauthorized person".[1] Within the context of this work, the concept of data protection is used to refer to the protection of the privacy of personal data or computerized information which relates to any identifiable individual from all forms of threats and abuses.[2] The concept of data protection arises from the fundamental human right to privacy.[3] For example, Article 12 of the Universal Declaration of Human Rights provides that:

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".[4]

▷ LL.B., BL., LL.M, PhD *cand.*, Barrister and Solicitor of the Supreme Court of Nigeria. The author is grateful to Ulrich Gasper for his comments on the earlier draft of this article. However, the author is solely responsible for the views expressed in this article and neither does the article represent the views of any national or international organization(s) that the author consults for or has consulted for or is affiliated to. Further information on the author on p. 128.

1 *See* The Blacks Law Dictionary (9th Edition, West Publishing: USA, 2009, p. 452).

2 Within the context "personal data" is used to classify any information which relates to an identified or identifiable individual who is the subject of personal data processing. *See* Article 1, Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, adopted at the 37th session of the Authority of ECOWAS Heads of State and Government, (Abuja, 16 February, 2010).

3 *See* Article 12 Universal Declaration of Human Rights. *See also* Article 8 of the Charter of the Fundamental Rights of the European Union (2000) O.J. (C. 364) 1, available at *http://www.europarl.eu/charter/pdf/text-en.pdf.*

4 *See* Article 12 United Nations Universal Declaration of Human Rights (1948).