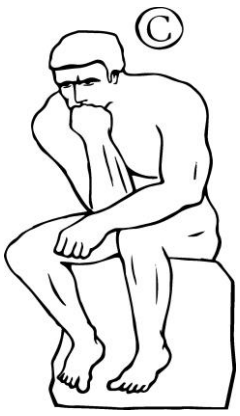
MARS-IP - NEWSLETTER

Nr 1 - 2018

SUMMARY



FOCUS ON DATA PROTECTION

Transmission of data from WHATSAPP to FACEBOOK

In 2014, WHATSAPP was acquired by FACEBOOK, Inc. On 25 August 2016, it published online a new version of the terms of use and confidentiality of its application, advising users of the now systematic transmission of their personal data to FACEBOOK, Inc. It was specified that this transmission had two purposes in particular, "*business intelligence*" and security. Users thus had the choice between refusing, their access to the application thus being blocked, or accepting unconditionally.

The Article 29 Working Party[1] or WP29, alerted by these changes, was quick to ask WHATSAPP to provide it with further information regarding said changes and demanded immediate suspension of all targeted advertising. Furthermore, it instructed its "*Enforcement Subgroup*" to coordinate future investigations by national authorities and in particular those of the National Data Protection Commission (hereafter, CNIL).

Throughout November 2016, the WP29 carried out inspections online and by questionnaire and summoned WHATSAPP to a hearing.

Through these various inspections, CNIL found that no information related to the processing of personal data established by WHATSAPP was present on the form to create an account in the application and that consent collected from old and new users concerning the transmission of their data to FACEBOOK, Inc. was not free.

With these findings, CNIL then urged WHATSAPP to send it samples of French users' data sent to FACEBOOK, Inc.

WHATSAPP only replied that it did not use French users' data targeted advertising purposes and categorically refused to disclose further information to CNIL, considering itself subject only to US law.

Also, on 18 December 2017[2], given WHATSAPP's non-compliance with its obligation to cooperate with CNIL (1.) and the violations related to data processing that it implements (2.), CNIL publicly put WHATSAPP on notice to comply with the law within one month (3.)… Read more on our website

[1] WP29 includes all of the European CNILs.

[2] https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000036232595&fastReqId=1869831892&fastPos=2

THE IMPACT OF THE GENERAL DATA PROTECTION REGULATION ON THE PROCESSING OF YOUR EMPLOYEES' DATA

The entry into force of the General Data Protection Regulation (hereinafter GDPR) on May 25 will have a significant impact for all organisations that collect, process and / or store personal data on European residents. Whatever the size or level of development (large corporations, SMEs, start-ups ...) as soon as the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in article 9.1 or personal data relating to criminal convictions and offenses referred to in article 10.

If the Data Protection Act (Loi Informatique et Libertés) applicable in France already constitutes an extremely protective framework for personal data (right of access to data, right of rectification and erasure...), the GDPR reinforces the rights of employees. The expression of consent is now precisely regulated, employees must be informed in a clear, intelligible and easily accessible way of the use of their data and must have a systematic possibility to give their unambiguous consent or to refuse it. These broad requirements will transform the organisation and management of employee data procedures and employee rights.

In this way, the GDPR grants a number of new rights to employees and imposes new obligations on employers, the greater part of which is extended to their processor(s), including:

- the right to data portability: any employee having transmitted data will have the right to recover it in an easily reusable form and to then transmit it to a third party/another controller;
- the reinforcement of confidentiality and data security: the employer, and its processors, is subject to reinforced security obligations and a requirement to notify any personal data breach to the supervisory authority within 72 hours;
- the prohibition of transmission by the employer of personal data of employees who are European citizens, outside the European Union, to countries where the protection of data is considered insufficient by the European Commission, cf. USA;
- impact assessments: companies wishing to process personal data shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data within the restrictions of the GDPR and in particular for risky processing operations;
- the right to restriction of processing: limiting the collection and retention of data to relevant information (smart data) only;
- systematic internal maintenance of a record of processing activities: the purpose of the GDPR is to simplify the preliminary steps and to make companies more accountable; therefore, it removes, with a few exceptions, the preliminary formalities (declarations and requests for authorisation) from supervisory authorities. Instead, companies must keep a record of processing activities in-house, which can be consulted at any time by the supervisory authorities;
- the designation of a data protection officer, who will be responsible for informing or advising the controller or his processor(s): for structures that handle sensitive or mass data this is a requirement; for others, a recommendation;
- recognition of the right to compensation: any employee who has suffered material or moral damage as a result of a violation of the provisions of the GDPR by the data controller or one of its processors will be granted a right to compensation.

In the event of a breach of the provisions of the new regulation by the employer or one of its processors, the GDPR provides for extremely heavy administrative sanctions, which may range from a fine of 4% of the annual turnover or the payment of the sum of 20 million euros, whichever is higher.

The sensible approach for employers to prepare for the coming into force of the GDPR:

- carry out an inventory of the processing of personal data implemented within the structure;
- evaluate the practices and procedures put in place;
- identify the risks associated with the processing operations implemented and plan the measures necessary for their prevention,
- always maintain and update documentation ensuring the traceability of the measures taken, as in the event of an audit by the competent authority or challenge by the employee, as it is now the controller, i.e. the employer and, where applicable its processor(s), on whom the burden of proof lies.

Although at first glance, compliance with the provisions of the GDPR may appear extremely restrictive, it has strategic value. In the long term, it will help to strengthen the trust of employees - and partners and customers - in the organisation concerned. It will also be an opportunity to strengthen the internal data security of the organisation. Finally, compliance will be rewarded by the award of one or more CNIL (the French national data protection authority) labels or of certification beneficial to the brand image and will thereby constitute a competitive advantage.

TRADEMARK LAW

General specifications concerning the EU Certification mark

The reform of European Union trademarks dated October 1st, 2017 has led to the introduction of a new type of European trademark: the certification mark. This is defined in Article 74(a) of Regulation (EU) 2015/2424 dated 16th December, 2015 as that "*which distinguishes the goods or services for which the material, the way in which the products are produced or the services supplied, the quality, precision or other characteristics with the exception of geographical origin, are certified by the proprietor of the mark in relation to the goods or services which do not qualify for such certification*". This type of trademark guarantees the use of the mark in relation to the certification standards defined by the applicant.

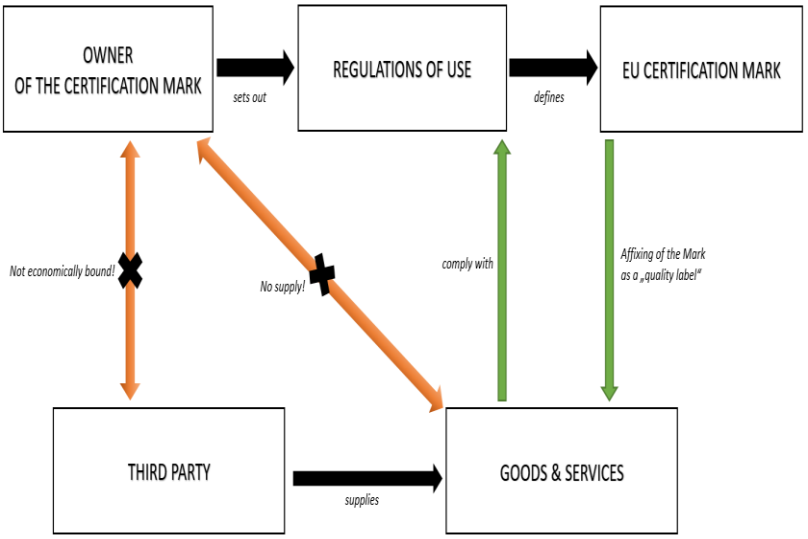
The certification mark benefits the consumer, since it enables more transparency with regard to the quality of the products and/or services and the owner, who thereby gives value to his engagement and offer and proves his neutrality on the market. As for the European Union Trademark, this new kind of mark applies to all 28 countries of the European Union. Thus, it enables owners to easily provide and control the use of their signs by third parties.

In a recent decision, the CJEU (June 8, 2017, C-689/15, W. F. Gözze Frottierweberei GmbH c/ Verein Bremer Baumwollbörse) ruled that an individual trademark cannot be used as a certification mark and could be subject to revocation since it was not put to genuine use by its owner. Indeed, due to the lack of regulation regarding certificates, a significant number of certifying bodies applied in the past for individual marks. However, since the above-mentioned decision of the CJEU, it is important to react quickly in order to avoid any application for revocation.

In fact, individual marks and certification marks have different functions, the former enable the consumer to associate a mark with its owner and the latter enable one to distinguish between goods and services, which have been certified from those which have not. It is interesting to note that the company BREMER BAUMWOLLBÖRSE GmbH, which was involved in the case cited above, applied for an EU certification mark on the very day that the reform introducing this type of mark entered into force.

At the time of writing this document, only a few certification marks have been filed, including well-known signs such as  or  . It seems therefore to be the perfect time to file an EU certification mark and benefit from a right of priority.

I. Who is able to file an EU Certification Mark?



Unlike the collective mark, which can be only filed by associations or state bodies, any legal or natural person may apply to register a certification mark.

However, the Office sets a limit under the title of "*duty of neutrality*", namely:

- the applicant should not carry out any business involving the supply of goods and/or services protected by the certification mark and
- the applicant and the third parties using the certification mark should not be economically bound (for example a branch office).

Hence, the applicant wishing to register a certification mark should provide a simple signed statement to the Office that he does not carry out any activity relating to the supply of the certified products and services.

II. The chosen sign must be distinctive

In the same way as for individual or collective marks, a certification mark has to be distinctive. However, in this instance, the function of the mark is not to distinguish the goods and services provided by a specific company but, as the Office mentions in its guidelines, "*to distinguish goods or services certified by one certifier from those that are not certified at all and from those certified by another certifier*". This point will certainly give rise to several interesting decisions in the future.

III. How does the owner set out the given standards for the certification?

Of course, the products and services to be certified have to be listed, just as for any individual or collective trademark.

The essential element of the certification is the regulation of use of the mark provided by the owner, which must be filed within two months at the latest from the date of application. This document defines objective conditions governing the use of the certification mark by a third party such as:

- the characteristics of the goods and services to be certified, e.g.:
    - persons or type of persons authorised to use the mark
    - quality of the goods and services
    - mode of manufacture
- the testing and supervision measures to be applied by the owner, namely:
    - control of the market by the owner or a third party
    - sanctions for non-compliance with the regulations of use
- the fees to be paid in connection with the use of the trademark by third parties, where applicable.

All these conditions have to be drafted with precision in order to be clearly understood by the market operators. The definition of the controls and sanctions operated by the owner is also important in order to dissuade incorrect use of the mark.

However, the Office clearly mentions in its guidelines as an absolute ground of refusal that "*an EU certification mark will not be capable of distinguishing goods or services certified in respect of the geographical origin*".

IV. Costs

The Office has based the fees for the application for an EU certification mark on the fees for the application for a collective mark, namely:

- basic fee for the application for an EU certification mark: **EUR 1,800.00**
- fee for the second class: **EUR 50.00**
- fee for each class exceeding two: **EUR 150.00.**

THE AUTHORS

Marie-Avril Roux Steinkühler

Partner

Dr. Marion-Béatrice Venencie-Nolte, LL.M.

Attorney

Marine Milochau, LL.M.

IP legal advisor

To contact us

MARS IP
Bleibtreustr. 20
10623 Berlin

+49 30 56 55 35 50
office@mars-ip.eu
www.mars-ip.eu

M.A.R.S.

IP