EUROPEAN
COMMISSION

Brussels, 10.4.2014
SWD(2014) 135 final

# COMMISSION STAFF WORKING DOCUMENT

## on the existing EU legal framework applicable to lifestyle and wellbeing apps

*Accompanying the document*

**GREEN PAPER**

**on mobile Health ("mHealth")**

{COM(2014) 219 final}

# Contents

## 1. INTRODUCTION

This Staff Working Document purports to give a non-exhaustive description of the EU legislation, which is applicable to lifestyle and wellbeing apps. This is a state of play of the applicable rules of EU legislation, since some issues concerning both the developers of apps and their users are still to be either defined or interpreted. It is to be noted that the fact that Union legislation could not yet address latest developments in this sector nor did the Court have the opportunity to clarify the applicability of existing legislation on these newly developed apps, still leaves room for interpretation.

The aim of this Staff Working Document is to provide simple guidance as to the EU applicable legislation. Where this is not yet possible because of the above mentioned reasons, the Commission services will not purport to provide any interpretation as this is the role of the Court of Justice of the European Union, as well as for any question of interpretation of EU legislation.

## 2. EU SAFETY AND PERFORMANCE REQUIREMENTS

Some mHealth apps may fall under the definition of a medical device or of an in-vitro diagnostic medical device and therefore may have to comply with the safety and performance requirements of Directive 93/42/EEC concerning medical devices or Directive 98/79/EC on in vitro diagnostic medical devices respectively.

On 26 September 2012, the European Commission adopted two Proposals, one for a Regulation on medical devices and the other for a Regulation on in vitro diagnostic medical devices which will, once adopted, replace the existing legal framework applicable to medical devices in the Union.

There are no binding rules in the Union as to the delimitation between lifestyle and wellbeing apps and a medical device or in vitro diagnostic medical device. Since January 2012, in order to help software developers and manufacturers identify whether their products fall or not under the Directive on medical devices or the Directive on in vitro diagnostic medical devices, the Commission's services have issued some guidance on this issue which will be continuously updated[1].

It is not yet clear if and to what extent lifestyle and wellbeing apps could pose a risk to citizens' health. However, when placing an app on the market, an app developer needs to know whether he has to comply with any Union safety requirements.

Due to the fact that both the General Products Safety Directive and the Directive on liability for defective products apply to manufactured products, it is not yet clear if and to what extent they apply to lifestyle and wellbeing apps.

[1] Guidelines on the qualification and classification of stand-alone software used in healthcare within the regulatory framework of medical devices, MEDDEV 2.1/6 January 2012

## 3. APP USERS' RIGHTS

### 3.1. Right to privacy and to data protection

Apps are able to collect large quantities of data (e.g. data stored on the device by the user and data from different sensors, including location) and process these in order to provide new and innovative services to the end user.

App developers, unaware of the data protection requirements, may create unwanted threats to the privacy and reputation of users of smart devices.

The relevant legal framework applicable is composed of the Data Protection Directive[2] and the ePrivacy Directive[3]. These rules apply to any apps installed/used by users in the EU, regardless of the location of the app developer or the app store[4].

*Data Protection Directive*

The national laws transposing the directive impose obligations on data controllers and data processors. Data controllers are natural or legal persons, which determine the purposes and means of the processing of personal data; whereas data processors are natural or legal persons, which process personal data on behalf of controllers.

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes, as well as adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

The legal ground for processing personal data varies according to the nature of the data processed as summarised below:

| **General data** | **Sensitive data such as data related to health** |
|---|---|
| Processing authorised for a legitimate purpose **such as**:<br>➢ the data subject has unambiguously given its consent;<br>➢ processing is necessary for contract performance;<br>➢ processing is necessary to comply with a legal | Principle of prohibition to process with limited derogations **such as**:<br>➢ the explicit consent of the data subject; except where in accordance with national law the prohibition to process such personal data cannot be lifted by the consent of the data subject;<br>➢ the vital interest of the data subject or of another person where the data subject is |

[2] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.OJ L 281, 23.11.1995, p. 31. It is currently under revision, see Commission proposal: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[3] DIRECTIVE 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as modified by Directive 2009/136/EC, OJ L.337, p11, 18.12.2009.

[4] Data protection rules are applicable not only when the data controller is established within the EU, but whenever the data controller uses equipment situated within the EU, such as smart devices, in order to process data (Article 4 of the Directive).

| | |
|---|---|
| obligation on the data controller;<br><br>➢ the legitimate interests of the data controller in so far as not overridden by the interests for fundamental rights and freedom of the data subject. | physically or legally incapable of giving his consent;<br><br>➢ where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, and where those data are processed by a health professional or any professional bound by the obligation of secrecy. |

Personal data concerning health includes information on both the physical and mental health of an individual. According to the Article 29 Data Protection Working Party[5] health data should cover any personal data closely linked to the health status of a person, such as genetic data or data on consumption of medicinal products or drugs.

Lifestyle and wellbeing apps can collect indifferently personal data of general nature (e.g. information on the data subject's hobbies) and health data (e.g. heartbeat or oxygenation of the blood).

The processing of personal data concerning health is in principle prohibited as these data are considered sensitive. However, such processing can be authorised in strictly limited circumstances (see table above).

One exemption to the prohibition to process data related to health is based on the performance of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services. This derogation requires that the processing is done by a health professional or any professional bound by the obligation of secrecy (Article 8(3) of the Directive). Other exemptions to the prohibition of the processing of personal data concerning health may be laid down by Member States, for reasons of substantial public interest, either by law or by decision of the supervisory authority, subject to suitable safeguards (Article 8(4) of the Directive).

The data subject's explicit consent to the processing of his health data must be freely given, informed and specific and cannot be considered as a blanket leave for the controller to process health data in breach of for instance the principle of purpose limitation.

Hence, data collected for the purpose of mHealth services cannot be further processed for commercial purposes, unless the data subject, duly informed, has specifically and explicitly consented to the processing of his data for those other commercial purposes. According to the principle of purpose limitation, aforesaid purpose must be specified, explicit and legitimate. The other principles relating to data quality (including data minimisation, data retention limitation and the adoption of appropriate safeguards in this regard) are applicable too (Article 6 of the Directive).

Data controllers must notify the relevant national data protection authorities before carrying out operations of processing of personal data (Article 18 of the Directive).

[5] Article 29 Working Party Working Document on the processing of personal data relating to health in electronic health records, 15 February 2007.

The Article 29 Working Party recently published an opinion "*on apps on smart devices"*, which seeks to clarify the legal obligations of each of the parties involved in the development and distribution of apps[6].

The Opinion offers some guidance to all the players, in particular the need to provide clear and unambiguous information about data processing to users (e.g. the types of data processed, the purposes for processing and data retention periods). It should be made available in a clear and unambiguous format prior to the installation of the app (e.g. in the description of the app on the app store) and apps/app developers should not alter the purposes or types of data collected without seeking further consent from the end-user.

In addition, whenever automated decisions are taken based on the compiled data, the data subject may obtain from the controller by way of an access request information about the logic behind those decisions (wording of Article 12 of the Directive). This might be the case when the user's performance or conduct is evaluated based on health data. Subject to user request, the app controller also must enable rectification, erasure or blocking of personal data if they are incomplete, inaccurate or processed unlawfully.

Furthermore, third parties may also be involved in the data processing of data related to health, for instance if the app developer has outsourced some or all of the data processing to a third party, which may thus assume the role of a data processor.

If the third party processes personal data for its own purposes, it may also be a joint data controller with the app developer. It must therefore ensure respect of all data protection principles, in particular the purpose limitation principle, and security obligations for the part of the processing for which it determines purposes and means. The respective responsibility of each party will have to be established on a case-by-case basis.

If the data processed by the third party are personal data related to health, it will have to obtain for the explicit consent of the user as the processing will be done for a distinct purpose than the one of the app developer. In accordance with national law there might also be cases where the prohibition to process sensitive personal data cannot be lifted at all by the consent of the data subject.

The level of complexity of identifying the role of a third party can be well illustrated by the case of cloud computing providers as they can according to the specific circumstances be either data processors or data controllers or both at the same time.

The Article 29 Working Party opinion on cloud computing[7] provides useful guidance on the application of existing data protection rules to cloud providers[8].

In the EU, the current Data Protection Directive[9] is being revised in order to better respond to challenges posed by the rapid development of new technologies and globalisation. The

---

6 Article 29 Working Party *"Opinion 02/2013 on apps on smart devices"*, 27 February 2013.

7 Article 29 WP "*Opinion 05/2012 on Cloud Computing*", 01.07.2012.

8 The guidance clarifies that a cloud provider can be either a data controller or data processor according to different circumstances, and also what is the law applicable in case the place of establishment of a cloud provider may be hard to determine.

9 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, L 281/31, 23.11.1995

proposal for a General Data Protection Regulation repealing the Data Protection Directive will prevent fragmentation in the way data protection is implemented across the European Economic Area, while ensuring legal certainty and a consistent and high level of protection of individuals[10].

*e-Privacy Directive*

The ePrivacy Directive[11] sets a specific standard to any entity worldwide that wishes to store or access information stored in devices of users located in the European Economic Area. Its main provisions are:

- Cookies. The storing of information or the access to information already stored in the terminal equipment of a user is only allowed on condition that he has given his consent, having been provided with clear and comprehensive information about the purposes of the processing (Article 5(3) of this Directive).

This consent requirement applies to any information (i.e. not limited to personal data as information can be any type of data stored on the device). This means that when installing an app, users should be given the choice to accept or refuse cookies or similar tracking technologies to be placed on their device.

It should be noted that this consent needs to be distinguished from the one given for authorising the processing of personal data as it relates to the purpose of storing information or gaining access to information already stored in the smart device. However, data controllers can collect consent for both processing operations at the same time, either during the installation or before the app starts to collect personal data from the device.

Data breach notification duty. It imposes an obligation on providers of publicly available electronic communications services (e.g. Telecom operators) to provide notice in the event of a data security breach.

### 3.2. Other rights

#### *3.2.1. Consumers' rights Directive*

When a consumer buys an app in the EU, the Consumer rights Directive[12] ensures a uniform EU-wide level of protection.

Traders have to comply with a series of requirements when a consumer buys a lifestyle and wellbeing app online (this purchase of an app is a "distance contract" under the directive).

Although the directive expressly excludes contracts for healthcare, the process of purchasing a lifestyle and wellbeing app cannot be considered per se a contract for the provision of healthcare. Therefore the directive covers lifestyle and wellbeing apps.

---

10 COM(2012) 11 final.

11 ePrivacy Directive 2002/58/EC, as revised by Directive 2009/136/EC.

12 Directive 2011/83/EC on consumers' rights.
This Directive repeals Directive 97/7/EC **as of 13 June 2014.**

The trader is considered to be either the app store (when the consumer downloads an app from an app store) or the app developers (in cases where the consumer buys the app directly from them).

Before the conclusion of a distance contract for the acquisition of an app, the trader has to provide the consumer with a series of information, in particular on:

- **the main characteristics of the app**
- **the identity of the trader and his contact details**
- **the total price and any additional charges of the app**
- the arrangements for payment
- **where a right of withdrawal exists, the conditions for exercising that right and the model withdrawal form**
- **where a right of withdrawal does not exist, the information on that fact or the circumstances under which the consumer loses his right of withdrawal**
- the duration of the contract and in case of an indeterminate duration the conditions for terminating the contract
- where applicable, the minimum duration of the consumer's obligations under the contract
- the functionality of digital content, including applicable technical protection measures
- any relevant interoperability of digital content with hardware and software that the trader has to be aware of
- any relevant codes of conduct.

The trader has to provide the mentioned information in a clear and understandable language and in a way appropriate to the means of distance communication.

This means that when the app is downloaded on a mobile phone, the limited size of the phone display may have an impact on the amount of information that should be provided prior to the conclusion of the contract. If the means of distance communication allows only for limited space or time to display the information, the trader must provide, on that particular means of communication, the most important pre-contractual information (presented in bold print in the above table) whilst making available the complete information through, for example, a hyperlink.

The consumer has a 14-day period to withdraw from the contract. However, the trader can offer the consumer an immediate performance of the contract to which the consumer must expressly consent before the withdrawal period has lapsed while acknowledging that he thereby loses his right of withdrawal.

After the conclusion of the contract and at the latest before the performance of the service begins, the trader has to provide, on a durable medium (e.g. an e-mail or a pdf file, but not a link to a website), a confirmation of the contract comprising all the information in the above table.

The trader has to inform the consumer directly before he places his order about the main characteristics, the total price, the duration and termination of the contract and the minimum duration of the consumer's obligations under the contract.

The trader has to ensure that the consumer explicitly acknowledges that the order implies an obligation to pay, by labelling the order button with words "order with obligation to pay" or an equivalent unambiguous formulation. If the trader does not comply with this obligation, the consumer is not bound by the contract.

### *3.2.2. Rights enshrined in eCommerce Directive*

The eCommerce Directive[13] mainly contains information requirements to be provided by service providers, being legal or natural persons, providing information society services[14].

App stores, which are selling lifestyle and wellbeing apps, are providing information society services, as they provide such services *"for remuneration, at a distance, by electronic means and at the individual request of a recipient of services"*. App developers, when they are directly selling the apps, are also providing information society services.

'Free' apps are also regulated as the directive covers any economic activity, including cases in which the remuneration is received from other sources, such as advertising.

Information society service providers must comply with the law of the Member State in which they are established as regards the setting-up and exercise of their information society activities.

This however does not preclude Member States to take any appropriate measure against the service provider established outside of the EU for reasons of public interest.

The eCommerce Directive lays down general information requirements which a service provider (e.g. an app store) has to provide before the recipient places his order (i.e. before buying the app). The main provisions are summarised below:

**General information to be provided:**

- name, address and e-mail address of the service provider
- price, tax and delivery costs
- the relevant trade register when applicable

**Information to be provided before placing an order:**

- the different technical steps for concluding the contract
- the technical means for identifying and correcting input errors

[13] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[14] An information society service is "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*".

| |
|---|
| ➢ the languages offered for the conclusion of the contract<br>➢ any relevant code of conduct<br>➢ the contract terms and general conditions must be made available in a way that allows the recipient to store and reproduce them |

As soon as the consumer has placed his order, the service provider has to acknowledge the receipt of the order.

The eCommerce Directive also provides for a framework of liability for intermediary information society service providers. Depending on the nature of their activities, app stores may be regarded as hosting service providers[15] as they provide storage of information provided by the app developer (i.e. information being the app itself).

In this context, the hosting service provider may not be held liable for the information stored at the request of the recipient of the service (i.e. the app developer or owner) on the condition that:

- the provider does not have the actual knowledge of an 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

- the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the information.

Whether these conditions are met, would need to be assessed on a case by case basis as there may be different solutions employed by app stores when providing a platform offering lifestyle and wellbeing apps.

### *3.2.3. Rights enshrined in Unfair Commercial Practices Directive*

The Directive on Unfair Commercial Practices[16] intends to maintain a consumer's freedom of choice by prohibiting unfair commercial practices by traders.

The directive applies to all business-to-consumer commercial practices, including the selling of lifestyle and wellbeing apps.

A commercial practice is considered unfair if it does not comply with the principle of professional diligence and is likely to distort the economic behaviour of the average consumer. In particular, commercial practices are unfair if they are misleading or aggressive:

| **Misleading**: | **Aggressive**: |
|---|---|
| ➢ practice which contains false information or is in its overall impression likely to deceive the consumer | ➢ practice which is likely to significantly impair a consumer's freedom of choice by harassment, coercion or undue influence |

[15] Article 14 of the eCommerce Directive

[16] Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market.

| | |
|---|---|
| ➢ practice which omits material information that the consumer needs to take an informed purchase decision, or by which a trader hides or provides such information in an unclear, unintelligible, ambiguous or untimely manner | |
| **AND** causes the consumer to take a transactional decision that he would not have taken otherwise. | |

This means that when promoting or selling their products, traders – app stores or app developers – have to avoid any practices which could mislead a consumer or which could compromise his freedom of choice.

Annex I of the directive contains a list of 31 practices which are in all circumstances considered unfair.

**Some examples of misleading commercial practices, which can be relevant with regard to lifestyle and wellbeing apps:**

- false claim on being signatory to a code of conduct or on the approval of the product by a public or private body (e.g. EC conformity marking)
- using trust or quality marks without the necessary authorisation
- false claims that a product is able to cure illnesses, dysfunction or malformations.