

## **SOCIAL MEDIA AND THE GDPR: CONSUMERS SHOULD EXPECT BETTER**

Market Watch study finds that the social media platforms examined are breaching the GDPR by not implementing privacy by default settings.

**Düsseldorf/Berlin, 2 October 2018 – New rights! More control? The EU’s General Data Protection Regulation (GDPR) has been in force since the end of May and has been designed to give consumers greater control over their data. A recent study by the Market Watch team “Digital World” at the Consumer Association of North Rhine Westphalia (Verbraucherzentrale NRW) reveals how social media platforms are putting the GDPR into practice. It is clear that the privacy policies of the eight platforms examined still give consumers little indication of how their data is used. Contrary to the requirements of GDPR, privacy by default settings are not the most privacy friendly ones.**

In Germany, 80 percent of people over the age of 14 have accounts on social networks such as *Facebook* and *Twitter\**, where they share personal photos, thoughts, information about their relationship or job status, etc. “This kind of personal data provides a lot of fuel for data-driven business models such as personalised advertising,” says Ricarda Moll from Verbraucherzentrale NRW’s Market Watch team. “It is therefore all the more important that users know exactly how their data is handled.” But how do networks such as *Facebook*, *LinkedIn* and *Snapchat* fulfil the stricter information requirements in practice? How do they implement the requirement of privacy by default? The Market Watch experts’ initial review reveals major problems.

### **NOT EVEN THE DEFAULT SETTINGS OFFER (DATA) PROTECTION**

Under GDPR, social media platforms have to program the default settings in such a way that no personal data is processed other than that which is really needed for the intended purpose. “This is especially important when it comes to social media, because very few people change the default or privacy settings,” explains Moll. The

study shows that many of the platforms examined have not implemented the GDPR rules in a way that protects users' data.

Only few of the social platforms reviewed restrict the visibility of users' posts, for example. On most platforms, these posts are public, which means that they can be seen by anyone, not just the contacts selected by the user. In the opinion of the Market Watch team, the majority of the platforms are breaching the GDPR in this respect.

## **DO CONSUMERS REALLY HAVE CONTROL OVER THEIR DATA OR IS IT JUST AN ILLUSION?**

All but one of the platforms examined use personal data for the purpose of personalised advertising. Furthermore, their default setting is for data to be used to monitor users' browsing behaviour (tracking data). In some cases, the user does have the option to subsequently limit this. The Market Watch team is particularly concerned that it is usually not possible to limit the actual user tracking itself. "This means that consumers cannot control how much the platforms know about them," complains Moll. "Instead, they can only restrict how the platforms are currently permitted to use this information. From a consumer protection perspective, users merely have an illusion of control."

Overall, the review found that most of the platforms are still very data-hungry, with all but two of them asking users to transfer contact data from their address book. The repeated requests and the formulations used in these requests give the impression that users have to grant access to the address book to be able to use the platform at all. By sharing their address book, however, users may be passing on the data of other users who have not necessarily consented, for example because they have consciously decided not to sign up to the network in question.

## **PRIVACY POLICIES ARE ANYTHING BUT CLEAR**

The report also found that privacy policies leave much to be desired. For example, most of them are vague about the period of time for which data is stored. One platform's policy referred to information being stored for "*different lengths of time*". And when it comes to the sharing of data, the majority of the privacy policies do not mention specific recipients but instead refer to general categories such as persons, companies or third parties. "Before sharing personal information, consumers need to know exactly who else can access this data," Moll explains.

Users need to be made aware of their rights vis-à-vis social media platforms. For example, they have the right to ask *Facebook* and the others what personal data they store. However, some of the platforms reviewed do not make this sufficiently clear to users.

## **A RIGOROUS APPLICATION OF DATA PROTECTION RULES IS REQUIRED**

The results of the Market Watch report highlight that consumers should expect better when it comes to data protection. "Platforms must be rigorous in how they apply the rules of GDPR, and the supervisory authorities must check that this is the case," states Lina Ehrig, Head of the Digital and Media Policy Team at the

Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband – vzbv). “This requires the supervisory authorities to have the necessary resources at their disposal so that they can enforce the law and, in individual cases, exercise the option of imposing significant penalties for infringements.”

**Platform selection and method:**

The study covered eight social media platforms (*Facebook, Instagram, LinkedIn, Pinterest, Snapchat, Twitter, WhatsApp, YouTube/Google*), whose apps were installed during the reported period from 15 June to 4 July 2018. All of the findings relate to the observations made during this period. Further details on the content and methodology of the study can be found (in German only) at <https://www.marktwaechter.de/digitale-welt/marktbeobachtung/soziale-medien-und-die-dsgvo>

Note: On some matters, GDPR leaves a great deal open to interpretation. The assessments made are based on a consumer-friendly interpretation of the new rules.

\*Bitkom (2018). *Social Media Trends 2018*. Downloaded from <https://www.bitkom.org/Presse/Anhaenge-an-Pls/2018/180227-Bitkom-PK-Charts-Social-Media-Trends-2.pdf> (in German only)

**Digital World Market Watch:**

Digital World Market Watch is an early warning system used by vzbv and the German consumer associations to monitor and analyse the digital market from the consumer’s perspective. Its work is based on consumer complaints, empirical studies and an interactive online portal. The Market Watch “Digital World” project also supports the work of supervisory and regulatory authorities such as the German Federal Network Agency (BNetzA). Digital World Market Watch is made up of five focal consumer associations, each of which focuses on a specific area of the digital market: Bavaria – digital services, Brandenburg – digital purchasing, North Rhine-Westphalia – user-generated content, Rhineland-Palatinate – digital goods, Schleswig-Holstein – telecommunication services. The Market Watch “Digital World” project receives funding from the German Federal Ministry of Justice and Consumer Protection (BMJV). [www.marktwaechter.de/digitalewelt](http://www.marktwaechter.de/digitalewelt) (in German only)

**Further information**

*Ute Böhm | Editor, Project Team “Market Watch Digital World”*

*Consumer Association of North Rhine-Westphalia*

*Phone +49 211 3809 459*

*ute.boehm@verbraucherzentrale.nrw*

*Timo Beyer | Project Manager, Team “Market Watch Communications”*

*Federation of German Consumer Organisations (vzbv)*

*Phone +49 30 25800 529*

*timo.beyer@vzbv.de*