While Northern European countries such as Norway, Iceland, Luxembourg and Denmark register the highest percentage of internet penetration (97-98%), Eastern Europe has one of the lowest among developed countries (74%). And, among all European countries, Portugal and Italy are the places where people spend most time per day on the internet (+6 hours on average).
Practically all digital consumers in this region have at least one social media account and have used social media in some form in the last month. Daily time spent on social media continues to rise. Unlike globally where social engagement is now mobile-first, PCs/laptops remain the primary device for internet users in this region looking to access social media.
SOCIAL MEDIA PENETRATION IN EUROPE

On certain major networks, users’ activities are becoming more passive in nature, as engagement with these platforms becomes more frequent but less prolonged, and as social networkers become more selective about where they share their personal content.

As in most marketers, Facebook remains in prime position within the social media industry followed by Youtube and an aggressive Instagram growth surpassing Twitter users.

**TOP 10 SOCIAL PLATFORMS**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Members</th>
<th>Visitors / Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td><img src="image" alt="Graph" /></td>
<td><img src="image" alt="Graph" /></td>
</tr>
<tr>
<td>Youtube</td>
<td><img src="image" alt="Graph" /></td>
<td><img src="image" alt="Graph" /></td>
</tr>
<tr>
<td>Instagram</td>
<td><img src="image" alt="Graph" /></td>
<td><img src="image" alt="Graph" /></td>
</tr>
<tr>
<td>LinkedIn</td>
<td><img src="image" alt="Graph" /></td>
<td><img src="image" alt="Graph" /></td>
</tr>
<tr>
<td>Twitter</td>
<td><img src="image" alt="Graph" /></td>
<td><img src="image" alt="Graph" /></td>
</tr>
<tr>
<td>Google+</td>
<td><img src="image" alt="Graph" /></td>
<td><img src="image" alt="Graph" /></td>
</tr>
<tr>
<td>Signal</td>
<td><img src="image" alt="Graph" /></td>
<td><img src="image" alt="Graph" /></td>
</tr>
<tr>
<td>WhatsApp</td>
<td><img src="image" alt="Graph" /></td>
<td><img src="image" alt="Graph" /></td>
</tr>
</tbody>
</table>

*DEFINITIONS:
Members - People who say they have an account on the platform in question.
Visitors / Users - People who say that, within the last month, they have visited or used a social network’s website or app via any device.
GDPR
Aggregation of personal data by large corporations not only breaches the privacy of individuals but also deprives them of the opportunity to benefit from the value of the data they generate.

In May 2018, enabled by the EU General Data Protection Regulation, EU residents will now be able to request corporations to provide their personal data in a machine-readable form.

This would make it possible for users to securely store personal data from diverse data sources and monetize it if they wish to. Companies will have to design "virtual wallets" so as to provide users total control over the attributes that they wish to share, thus making it possible to derive monetary value from their data without compromising on their privacy.
**EU DATA PROTECTION**

**BEFORE MAY 25TH, 2018 - DPD**

Under the DPD, personal data was defined as data such as names, photos, email addresses, phone numbers, addresses, and personal identification numbers (social security, bank account, etc.).

**AFTER MAY 25TH, 2018 - GDPR**

Under the GDPR, personal data is defined as any information that could be used, on its own or in conjunction with other data, to identify an individual. This data includes IP addresses, mobile device identifiers, and geolocation and biometric data as well as data related to individual’s physical, psychological, genetic, mental, economic, cultural, or social identity.

The GDPR applies to personal data of subjects located in the EU, even if the companies processing or collecting data are not established in the EU. It is indeed a worldwide law.
GDPR: USERS

GDPR is empowering digital users allowing them to either leverage their own data for public or block them. Consumer attitudes towards sharing their personal information have become significantly more positive, they are open to it being used as part of everyday life as long as they can trust the company (see next slide).

Otherwise, to further bolster their privacy, users may take the following steps:

1. **Right to Access**: the right to obtain from data controllers information on how their data is being used, where, and for what purpose
2. **Right to be Forgotten**: If a person submits such a request, data controllers must erase all the requestor’s personal data, cease further use of that data, and if applicable, halt any third-party use of that data.
3. **Usage of Tracker Blockers**: Users may use browser extensions or add-ons which prevent their browsing activity from being tracked.
4. **Turn off Data Sharing with Advertisers**: The privacy settings on several online services give users the option of stopping their personal data from being shared with advertisers.
5. **Explore Privacy-Friendly Browsers and Search Engines**: Websites would still be free to send cookies to your browser, making it possible for the website to keep track of past visits and activity.
Key Findings on Sharing Personal Information
• For every 1 person who says they prefer not to share (36%), there are 2 who are either happy to if the need is explained (42%) or are happy to share if they trust the company (21%)
• By contrast, 6 out of 10 are only vaguely aware (24%) or not aware at all (38%)

Key Findings on App-Tracking
• 4 out of 10 consumers (39.4%) say they would prefer not to be tracked online and by apps and avoid opting-in (as is their right under the ePrivacy Directive)
• Nearly 1 in 6 (17.2%) say they avoid sites and apps which they know are tracking them

Key Findings on Personalization
Consumers notice when their devices and the services they are accessing seem to reflect who they are:
• For nearly 2/3 (64.4%), it is awareness of their location which is most evident
• Consumers rate personalized services most highly which are based around convenience:
  ▪ Autofill (3 out of 5)
  ▪ Personalized content (2.92)
  ▪ Being recognized by the brand (2.91)
• Location-aware services scored lowest with a score of just 2.59

Key Findings on Ad Blocking Software
• 1/3 (36%) of consumers already make use of ad blocking software and more than half (55%) are considering it. NOTE: Ad blocking is most commonly used on PC/Laptop devices rather than mobile.
• However, while using a private browser window may have the same effect as ad blocking software, only one quarter of consumers (25%) currently make use of this option.
Profiling, or developing a snapshot of an individual’s preferences using browser history, purchase history, and other related activity will no longer be acceptable under the GDPR unless the individual in question has explicitly consented.

If an organization outsources data entry or analysis to a third party or processes data on behalf of another organization, both parties are required to abide by the GDPR and are liable for violations.

The controller or processor must appoint a data protection officer when its core activities involve “regular and systematic monitoring of data subjects on a large scale.” The data protection officer will serve as a central point of contact who knows about how the collection or processing of personal data is performed. Other tasks include:

- **Privacy by design**: They should consider the privacy of collected data at all steps in the development of business concepts, from the very beginning, and discard personal data when they are no longer used.
- Data controllers must notify their supervisory authority and individuals affected by a personal data breach within 72 hours of learning about the breach.
GDPR: BUSINESS QUESTIONS

• How can individuals give consent in a legal manner?
• What is the process if an individual wants his data to be deleted?
• How will you ensure that it is done across all platforms and that it really is deleted?
• If an individual wants his data to be transferred, how will you do it?
• How will you confirm that the person who requested to have his data transferred is the person he says he is?
• What is the communication plan in case of a data breach?
• Why exactly are we archiving this data instead of just erasing it?
• Why are we saving all this data?
• What are we trying to achieve by collecting all these categories of personal information?
• Is the financial gain of deleting this information greater than encrypting it?
NEXT STEPS

✓ Incorporate data protection risk into the corporate risk management and internal control framework.
✓ Assess the categories of data held, where it comes from and the lawful basis for your processing. Map data flows into, within and from your organization.
✓ Create Article 30 documentation – the record of personal data processing activities drawn from the data flow audit and gap analysis.
✓ Assess the principle of data protection by design and by default.
✓ Be consumer centric: Provide more information to users on how data are collected and what are used for, even if the audience is not data savvy. As a best practice, it's recommended to include an extended FAQ for data methodology and usage.
✓ Plan how to recognize and handle data access requests and provide responses within a month.
✓ Remove and avoid collecting data of those below 16 years old. (Crimson might help with age filtering).
✓ Schedule regular audits of data processing activities and security controls. Keep records of personal data processing up to date.
✓ **Unbundled**: Consent requests must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service.

✓ **Active opt-in**: Pre-ticked opt-in boxes are invalid – use unticked opt-in boxes or similar active opt-in methods (e.g. a binary choice given equal prominence).

✓ **Granular**: Give granular options to consent separately for different types of processing wherever appropriate.

✓ **Named**: Name your organization and any third parties who will be relying on consent – even precisely defined categories of third-party organizations will not be acceptable under the GDPR.

✓ **Easy to withdraw**: Tell people they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw as it was to give consent. This means you will need to have simple and effective withdrawal mechanisms in place.

---

**NEXT STEPS: USER EXPERIENCE CHECKLIST**

**Communication preferences**

- SMS
- Email
- Social media
- Push notification
- Mobile app notifications
- Display advertising
- Banners
- Email newsletters
- Direct mail
- Telephone calls
- Text messages

**Privacy Policy**

- Data Protection
- Terms & Conditions
- Collection Notices
- Business Orders

**Keep in touch with us**

Please tick the boxes below to tell us all the ways you would prefer to hear from us:

- Yes, please, I would like to receive communications by email
- Yes, please, I would like to receive communications by telephone
- Yes, please, I would like to receive communications by mobile (text message)
- No thank you, I do not wish to receive communications

**Data Protection**

- Please provide your consent to the processing of your personal data.
- I agree to the terms & conditions.

**Terms & Conditions**

- Terms and conditions – website usage
- Privacy
- T&Cs
- Collection Notices
- Business Orders

**Copyright**

2018 Sickweather Inc. | 300 E. 39th St. Kansas City, MO 64111 | www.sickweather.com | 443-918-SICK
- **GWI Social Summary Q3 2017**, PDF published by Global Web Index

- **Digital in 2017: Western Europe**, PDF published by We Are Social and Hootsuite

- **Countdown to the EU GDPR**, article by itGovernance

- **The data protection directive versus the GDPR: understanding key changes**, article by GDPR:Report

- **Privacy in the Age of Data Aggregation**, article published by VALID

Sickweather knows where sick people are as the world’s first real-time map of sickness and the largest crowdsourcing community of its kind – processing millions of illness reports each month.

At Sickweather, our mission is to provide the most accurate, predictive and meaningful sickness forecast in the world to consumers and businesses alike. Our clients include some of the biggest names in pharmaceuticals, insurance, retail, household hygiene, and OTC. We envision a world in which Sickweather’s responsible and open curation of both clinical and anecdotal sickness data will create a singular, trusted global health surveillance system for the purpose of reducing healthcare costs, preventing hospital re-admissions, and decelerating the spread of illness.

Download the free Sickweather app:
iOS: http://sick.io/ios
Android: http://sick.io/android

Register for a free trial API key:
http://enterprise.sickweather.com

Test drive the Sickweather Pro analytics dashboard:
http://www.sickweather.com/pro