



# SO Connect is fully GDPR compliant

For the past 5 years, SO Connect has been building a network of SO WIFI hotspots and Beacons that generates a unique consumer profile database by combining proprietary offline data with online consumer profiles. As we deal with large amounts of data, we have significantly invested to ensure that our processes and procedures are compliant with the new General Data Protection Regulation (GDPR) which comes into effect in May 2018.

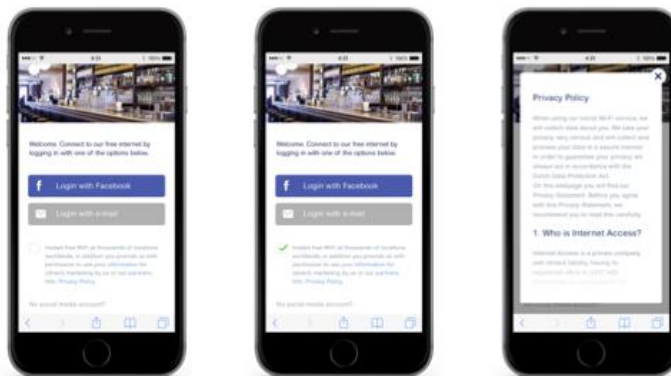
GDPR is a regulation that requires all businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. And non-compliance could cost companies dearly

Together with leading privacy lawyers at SOLV, we have implemented numerous changes over the past year to be fully GDPR compliant:

- New log-in portal and opt-in to obtain users' consent to process data
- Improved privacy policy
- New data breach protocol
- New data privacy and security process manual
- Enhanced data security and storage measures
- Appointment of an independent Data Protection Officer
- We deleted all data of users under 16 years old
- New opt-out page [sowifi.com/opt-out](http://sowifi.com/opt-out)

## How we at SO Connect obtains users' consent to process their data.

According to GDPR, Consent remains one of six lawful bases to process personal data. Consent is however only valid if *"freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."* (Art 4.11 GDPR)



Together with SOLV we adapted our log-in process more than a year ago to be GDPR ready. Our current opt-in is fully in line with the GDPR definition of consent, namely:

- **Freely given:** Historically we always provided the location owner with the choice whether they wanted to make it mandatory for the user to provide data in exchange for using the SO WIFI service, or allow a skip-login option. GDPR however indicates that tying the provision of a



service to a request for consent to process personal data that is not necessary for the performance of that service, is not considered valid consent. This means that we have needed to implement a skip-login option in all portals, allowing users to continue with the SO WIFI service even if they do not allow us to process their data.

- **Specific:** GDPR states that any consent should be given for a specific usage of the data, and if a company intends to use the data for multiple purposes it will also need to obtain multiple consents. We have therefore chosen to limit the usage of our data to “(direct) marketing” purposes. This term is still broad enough for us to continue to offer innovative products, while also informing our users of the specific purpose we intend to use their data for.
- **Informed:** Transparency is one of the fundamental principles of GDPR. For consent to be informed, it is necessary to inform the user of certain elements that are crucial for them to make a choice to share their data. This includes:
  - The controller’s identity; this is why “us” is clickable in the opt-in text where we explain who Internet Access BV is and how it relates to SO WIFI
  - The purpose for collecting the data: this is defined in the opt-in text as “(direct) marketing”. We have tried to be even more transparent and under the clickable “partners” we explain for each category of partners what kind of (direct) marketing they could expect.
  - What type of data will be collected and used: this is why “information” is clickable in the opt-in text where we explain what different types of data we collect depending on the log-in method chosen.
  - We have further included a link to our privacy statement during the log-in process and available on our website. In this privacy statement we explain how a user can request and opt-out or request us to delete all their data. We have made the process of opting-out just as simple as opting-in, as per GDPR requirements.
- **Affirmative action:** GDPR requires users to give an unambiguous indication signifying the agreement to the processing of personal data relating to him or her. In an online environment this means a tick-box which has not been prefilled.