# GDPR
## CHEAT SHEET

OnePageCRM

GDPR non compliance fine - Up to €20 million, or 4% annual global turnover – whichever is higher.

**In Place from 25 May 2018**

### LAWFUL PROCESSING (PICK 1)

1. **Explicit Consent (Marketing)**
2. **Performance of Contract**
3. **Legitimate Interest**
4. Vital Interest of Individual
5. Public Interest - Official Authority
6. Legal Obligation

### INDIVIDUAL RIGHTS

- Right to Access (Subject Access Rights)
- Right of Rectification (correction
- Right of Erasure (to be forgotten)
- Restriction of Processing
- Right to object to processing
- Right to Portability of your data
- Right over automated decisions and profiling

### CONSENT

When consent is used as a legal basis for processing, it should be:

- freely given
- Informed
- provided with clear affirmative action (no pre-ticked check boxes)
- as easy to withdraw as it was given
- specific to the purpose for which it was given
- unambiguous
- provable

### LEGITIMATE INTEREST

Three part test:

1. Identify a legitimate interest;
2. show that the processing is necessary to achieve it; and
3. balance it against the individual's interests, rights and freedoms.

The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.
You must include details of your legitimate interests in your privacy information.

### DIRECT MARKETING

The GDPR states that the processing of personal data for direct marketing purposes may be carried out for legitimate interest if you:

- have a relevant and appropriate relationship with them
- show that there is a balance of interests between the organisation and the person receiving the marketing.
- tell them you are going to market to them
- show them how to opt out of receiving marketing from you

### GDPR TERMS

**Controller**
The entity that determines the purposes, conditions and means of the processing of personal data

**Processor**
The entity that processes data on behalf of the Data Controller

**Data Subject**
A natural person whose personal data is processed by a controller or processor

**Personal Data**
Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

*Name*
*ID Number (s)*
*Home address*
*Phone numbers*
*Payment information*
*Email address*
*Website session ID*
*IP Addresses*
*Cookies*

**Special Category Data**
Can only be processed with explicit consent. Higher risk, store with caution.

*Racial or ethnic origin*
*Political opinions*
*Religious or philosophical beliefs*
*Trade union membership*
*Genetic data*
*Biometric data*
*Health /sex life/or sexual orientation*