

# PROJECT MOORE

19 JANUARY 2018

## PROJECT MOORE LAUNCHES ASK MOORE: AN INTERACTIVE PRIVACY TOOL



### MANAGE YOUR ACTIONS ON TONS OF PRIVACY TOPICS CATEGORISED IN EASY, FAMILIAR, AND CONCISE CHALLENGES.

We are happy to announce [Ask Moore](#): an exclusive interactive tool for improving privacy compliance. Ask Moore provides information about the General Data Protection Act (GDPR), and more. Rather than being merely a static guide or handbook about the GDPR, Ask Moore includes challenges that organisations are likely to encounter during a compliance trajectory and practical solutions on how to deal with them. These solutions can be generated into a personalised action list for organisations.

- more than 64 actions have been incorporated in Ask Moore devised in 4 project phases;
- Ask Moore includes more than 24 specific challenges;
- 16 clients have beta-tested Ask Moore; and
- 12 is the growing number of privacy topics.

“Many of our clients find it challenging to implement the requirements of the GDPR into practice,”

says Lieneke Viergever, one of Project Moore’s founders.

“They often lack the tools to keep track of and properly follow-up on the actions. To meet these challenges and help our clients achieve an appropriate level of compliance by 25 May 2018 and thereafter, we have developed Ask Moore for our clients.”

If you are interested in using the tool, please contact us at [info@projectmoore.com](mailto:info@projectmoore.com).

1. **How to?**  
Many of our clients find it challenging to implement the requirements of the GDPR into practice. They often lack the tools to keep track of and properly follow-up on the actions. This is why we have developed Ask Moore. We have translated the GDPR into clear-cut, business-focused actions. We hope Ask Moore will help you to become compliant in an effective way.

2. **Information obligation**  
The GDPR requires controllers to provide data subjects with information regarding the processing of their personal data.

3. **Lawful basis**  
Processing personal data requires at least one of the six lawful bases. A lawful basis is the reason why you are permitted to process personal data. Prime reasons for processing are, that processing: (i) is necessary to 'perform a contract' with the data subject, (ii) is in your 'legitimate interest', or (iii) started after having obtained the data subject's 'consent'.

4. **Consent**  
Consent is one of the six legal bases in the GDPR that legitimises the processing of personal data. And it's a gateway through specific types of processing (incl. special data and automated decision-making). At face value, consent may seem an easy way to establish a lawful basis for processing. However, obtaining and maintaining valid consent under the GDPR can prove to be a challenge as a result of the strict requirements. On the other hand, if consent is applied correctly, it will put individuals in control over their personal data.

5. **Record keeping obligation**  
The requirement for data controllers to notify supervisory authorities of their data processing activities has been removed under the GDPR. Instead, most controllers/processors will be required to maintain a record of their processing activities. The record must be made available to the supervisory authority on request. This topic addresses the challenges controllers and processors may experience in relation to the record keeping

6. **Data protection impact assessment ("DPIA")**  
A Data Protection Impact Assessment ("DPIA") is a process designed to assist organisations in identifying and minimising the privacy risks of new projects or policies.

*An overview of privacy topics.*

7. **Data protection officer ("DPO")**

Data protection officers are an important part of the accountability principle. The DPO is responsible for monitoring compliance with the GDPR, providing information and advice to the respective organisation, and liaising with the DPA.

Related Topics

- > 5. [Record keeping obligation](#)
- > 6. [Data protection impact assessment \("DPIA"\)](#)
- > 9. [Data subject rights](#)

Challenges

7.1 **Is your organisation required to appoint a DPO?**

7.2 **How should a DPO function in your organisation?**

7.3 **Should you voluntarily designate a DPO?**

7.1 **Is your organisation required to appoint a DPO?**

Sources: Art. 37(1) - (4) GDPR, Recital 97 GDPR, WP29 - Guidelines on Data Protection Officers

ADD ALL TO ACTION LIST

ACTION 7.1.1

ADD TO ACTION LIST

Phase: Inventory

*All topics have extensive practical information on privacy.*

← Action list

INVENTORY DESIGN IMPLEMENTATION REVIEW

## 7.Data protection officer ("DPO")

7.1 Is your organisation required to appoint a DPO?

If your **core activities** consist of **regular and systematic monitoring** of data subjects on a **large scale**, you should designate a DPO.

The threshold for what is considered **regular and systematic monitoring** is quite low (see [WP29 - Guidelines on Data Protection Officers](#)). Regular is described as 'recurring or repeated at fixed times', and 'systematic' is described as 'occurring according to a system'.

**Large-scale data processing** is a considerable amount of personal data at regional, national or supranational level, which could affect a large number of data subjects. WP29

Progress: 67%

Total actions:	3
Completed:	2
Open:	1

[Need help?](#)

Give us a call at +31 20 5200 870

*Every organisation has their own action list.*

For press inquiries, get in touch with:

## AUTHOR



**LIENEKE VIERGEVER**

Partner

[lieneke.viergever@projectmoore.com](mailto:lieneke.viergever@projectmoore.com)