What Is The GDPR…

And What Does It Mean For Data Privacy Protection At Your Agency?

JOHN KELLEHER
GENERAL COUNSEL, HUBSPOT

HubSpot
PARTNER DAY 2017

#INBOUNDPARTNERDAY

PANELISTS

Karen Neuman

Partner, Goodwin Procter LLP

Former Chief Privacy Officer, U.S. Department of Homeland Security

Adriano Tagliarina

CEO/Owner
Trialta GmbH

Gant Redmon

Program Director,
Cyber Security and Privacy
IBM

1 What Is The GDPR?

Brief History

EU adopted the **Data Protection Directive (DPD) in 1995**

- Protects EU citizens' fundamental right of privacy
- Covers all data related to a living person
- EU member states drafted local legislation to give effect to the goals of the DPD

Brief History

- DPD forbids sharing of personal data beyond the EU without adequate protection
- DPD sets out the 8 data protection principles (which the GDPR builds on)
- US – EU Safe Harbor used to meet “adequate protection”; invalidated in Nov 2015 and replaced by Privacy Shield in July 2016.
- **General Data Protection Regulation** adopted in June 2016; **compliance is required by May 2018**

2 What Should I Be Doing Now?

1

Determine Whether The GDPR Applies To You

2

Nominate a GDPR DRI

3

Assess Your Contacts Database

4

Improve Notice and Consent Now

5

Consider How and Where You Collect, Store and Share Personal Data

OTHER CONSIDERATIONS

- DPO and DPIA
- Privacy by Design and Privacy by Default
- Data Portability and The Right To Be Forgotten
- Security, Access Requests and Breach Notification
- Legal Documentation: Contracts, Privacy Notices and Internal Policies

3 HubSpot and GDPR

Our Strategy

Product Features

Education and Documentation

Maintain Means To Transfer Outside EU

HubSpot
PARTNER DAY 2017

Product Features

Forms: Display Privacy Notices and Establish Consent

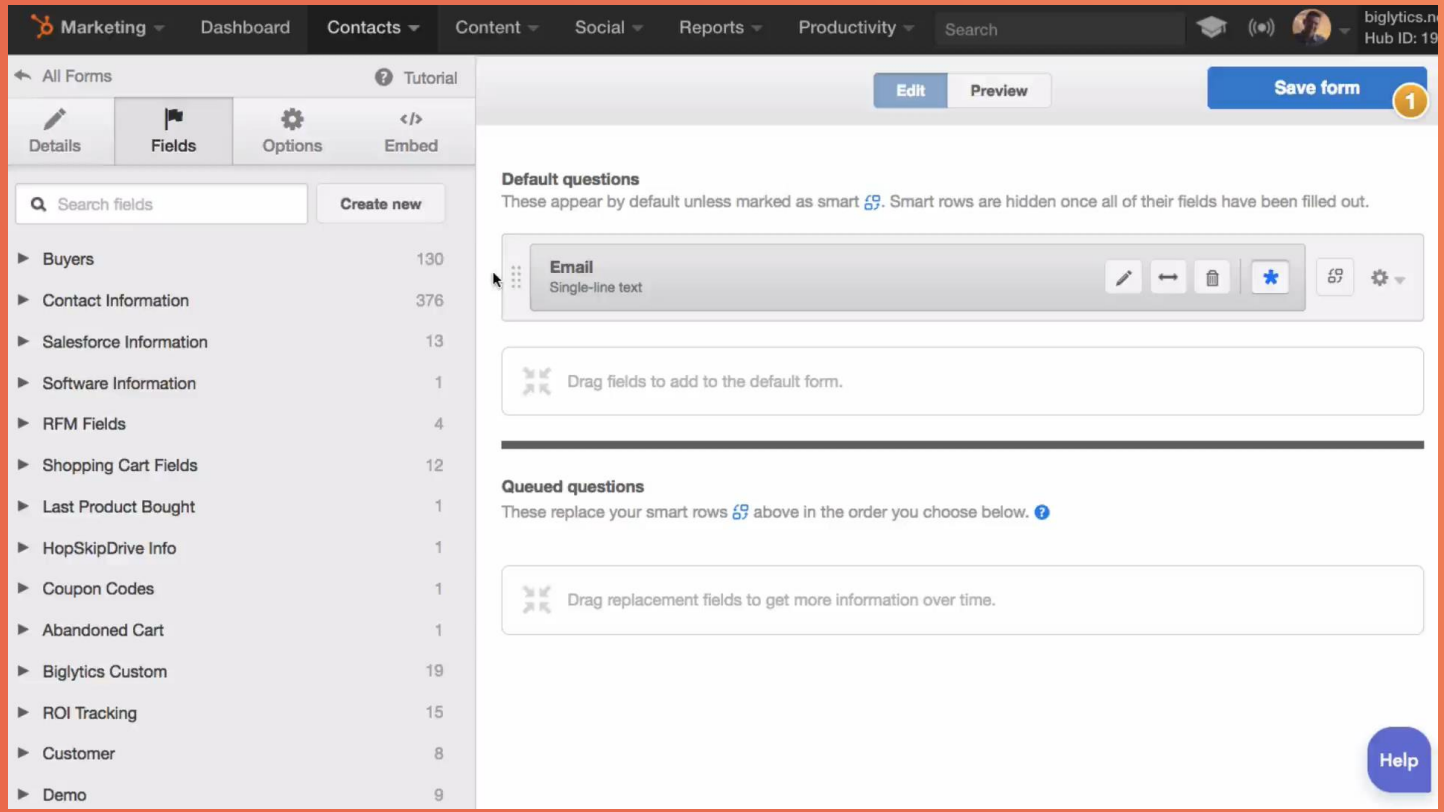
Contacts: Tracking Consent and Exporting Records

Email: Double Opt-In and Unsubscribe

HubSpot
PARTNER DAY 2017

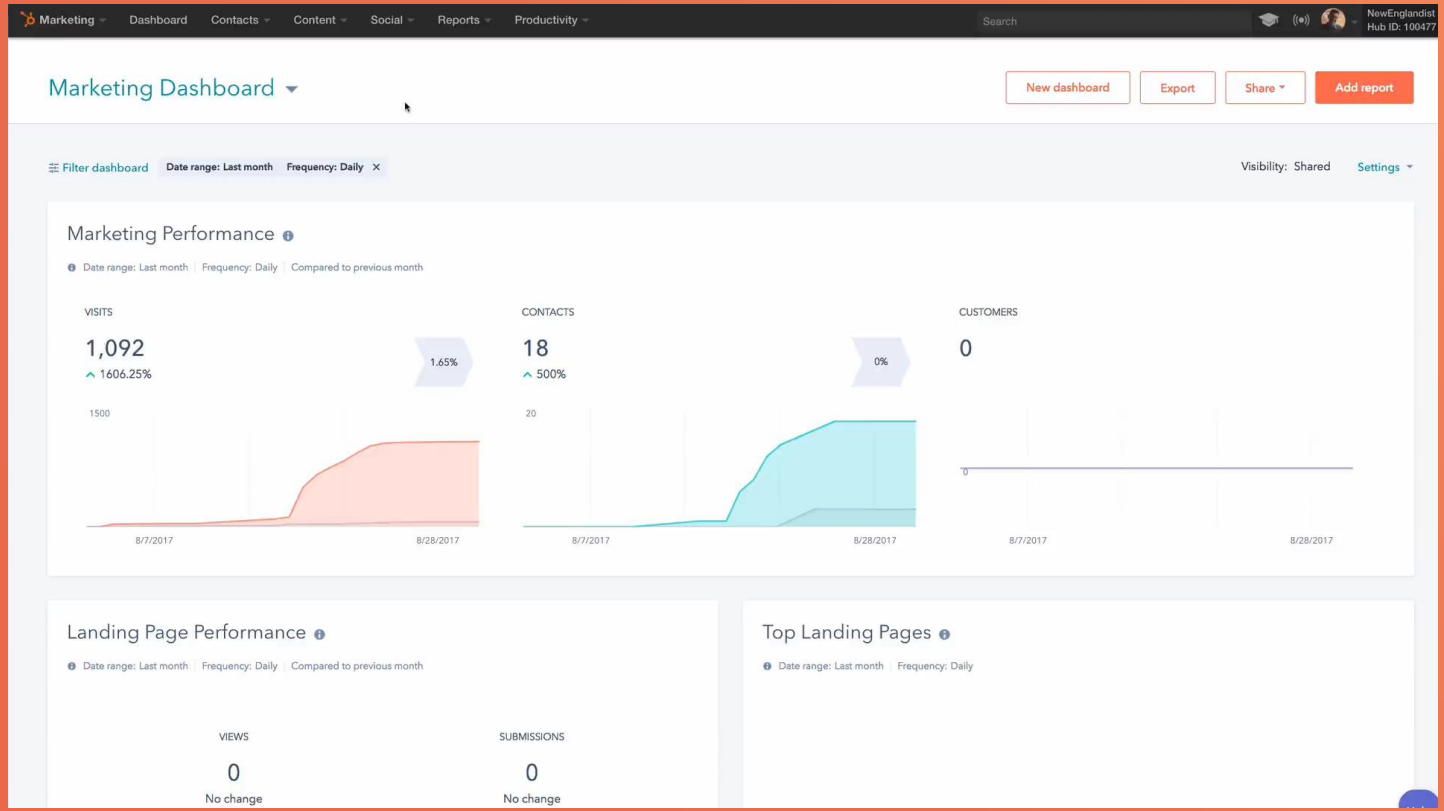
Existing Product Features:

Forms + Tracking Consent



Existing Product Features:

Double Opt In

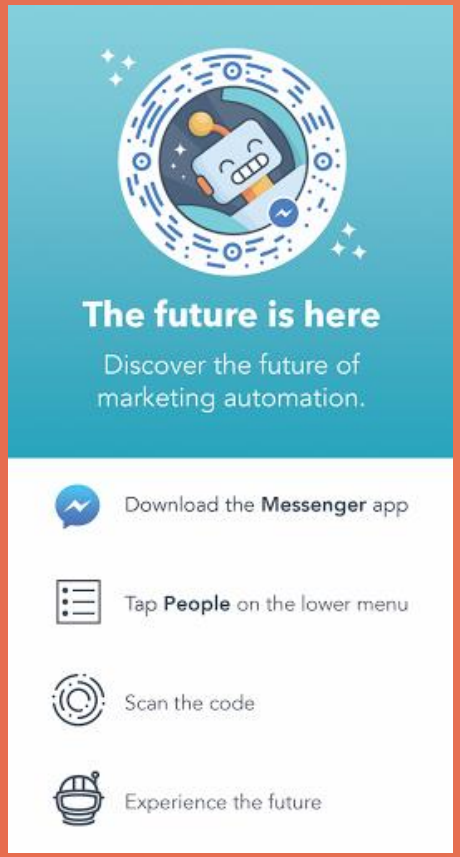


Product Enhancements

Motion.ai

+

HubSpot

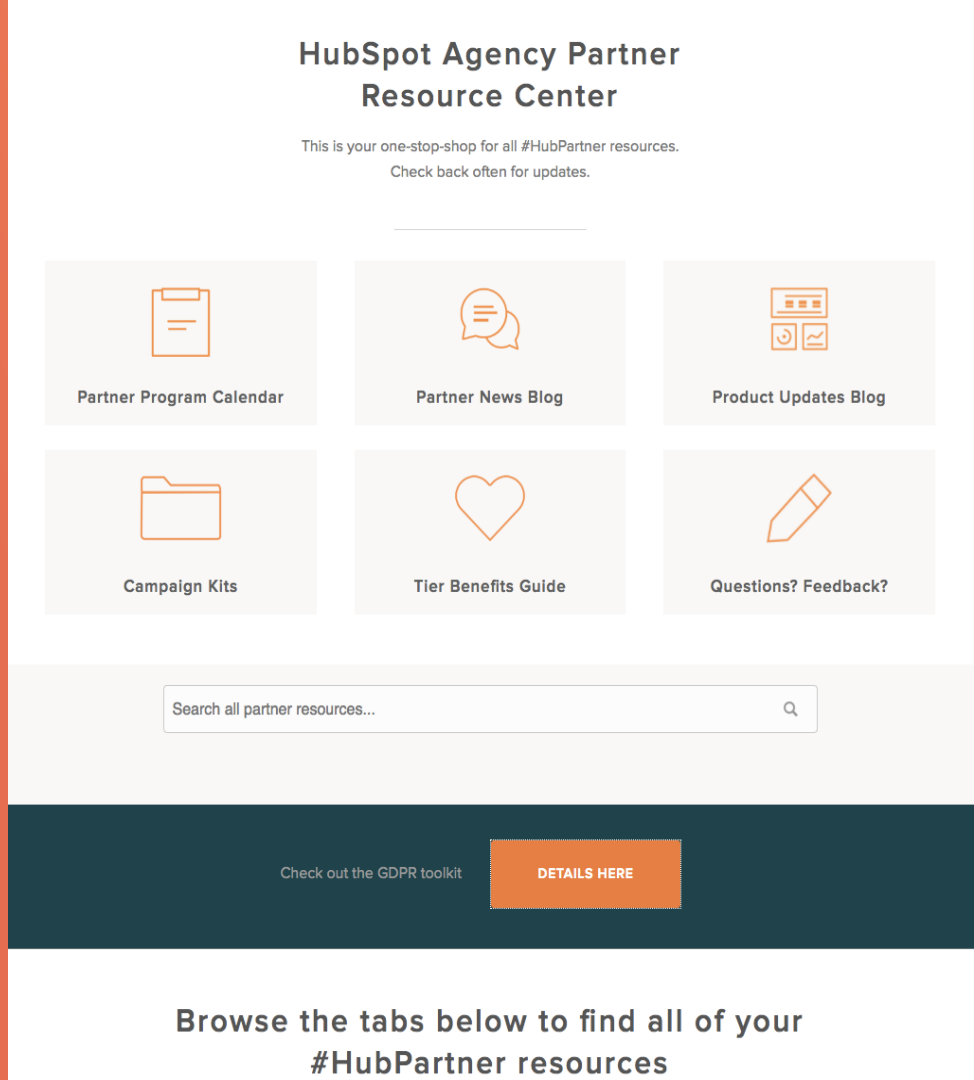


Education and Documentation:

Partner Resource Center

- Check out the news blog
- Subscribe for periodic updates
- Filter for GDPR, email notification

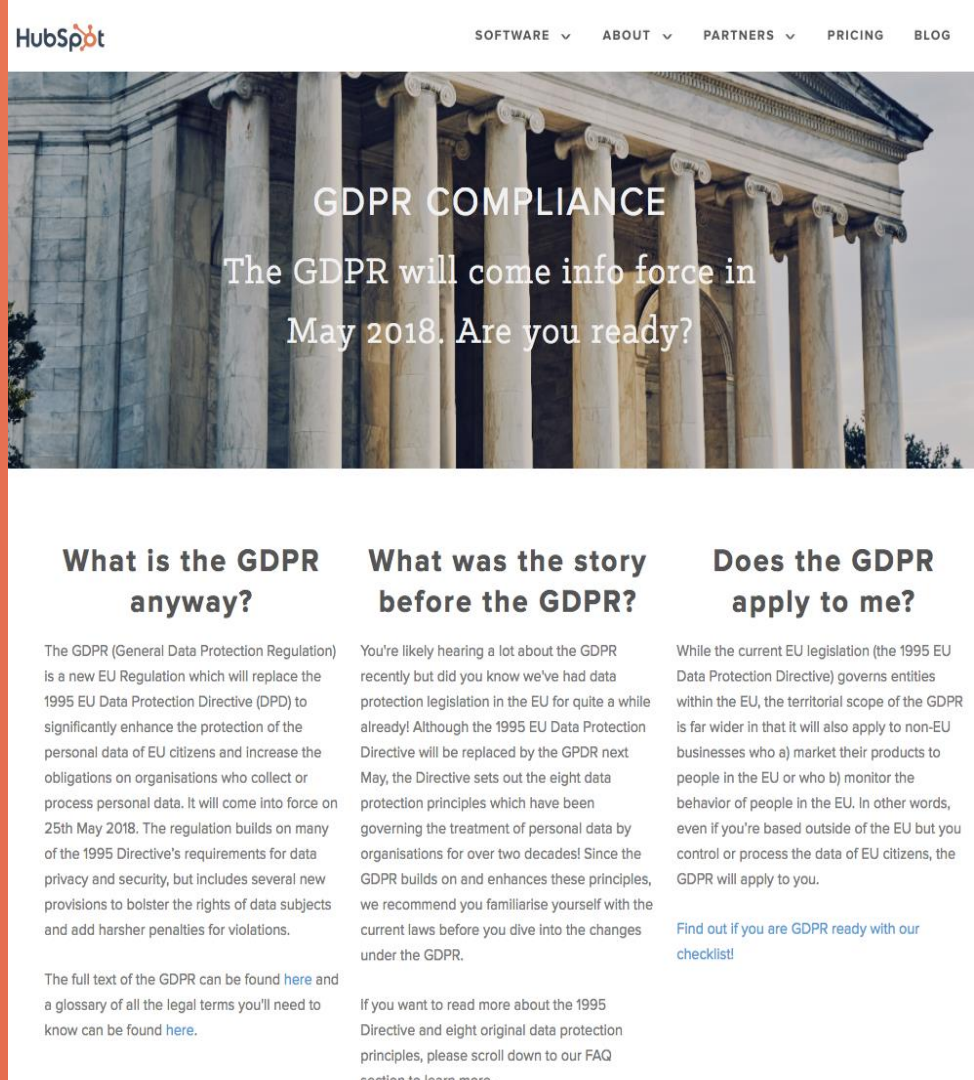
#gdpr Slack channel now live in HubSpot Partner Slack Group



Education and Documentation:

GDPR Compliance Toolkit

- hubspot.com/dataprivacy/gdpr



Education and Documentation:

GDPR Checklist

- hubspot.com/dataprivacy/gdpr

Since every business is different and the GDPR takes a risk-based approach to data protection, companies should work to **assess their own data collection and storage practices** (including the ways they use HubSpot's marketing and sales tools), seek their own legal advice to ensure that their business practices **comply with the GDPR**. In determining your next steps, here are some of the questions you should consider.

THE ASSESSMENT | THE GDPR PROJECT PLAN | THE PROCEDURES AND CONTROLS | THE DOCUMENTATION

The Assessment

- What personal data do we collect/store?
- Have we obtained it fairly? Do we have the necessary consents required and were the data subjects informed of the specific purpose for which we'll use their data? Were we clear and unambiguous about that purpose and were they informed of their right to withdraw consent at any time?
- Are we ensuring we aren't holding it for any longer than is necessary and keeping it up-to-date?
- Are we keeping it safe and secure using a level of security appropriate to the risk? For example, will encryption or pseudonymisation be required to protect the personal data we hold? Are we limiting access to ensure it is only being used for its intended purpose?
- Are we collecting or processing any special categories of personal data, such as 'Sensitive Personal Data', children's data, biometric or genetic data etc. and if so, are we meeting the standards to collect, process and store it?
- Are we transferring the personal data outside the EU and if so, do we have adequate protections in place?

The GDPR Project Plan

- Have we put a project plan together to ensure compliance by the May 2018 deadline?
- Have we secured buy-in at executive level to ensure we have the required resources and budget on hand to move the project forward?
- Do we require a Data Privacy Impact Assessment?
- Do we need to hire a Data Privacy Officer?
- Are we implementing a policy of 'Data Protection by Design and Default' to ensure we're systematically considering the potential impact that a project or initiative might have on the privacy of individuals?
- Have we considered how we handle employee data in our plan?

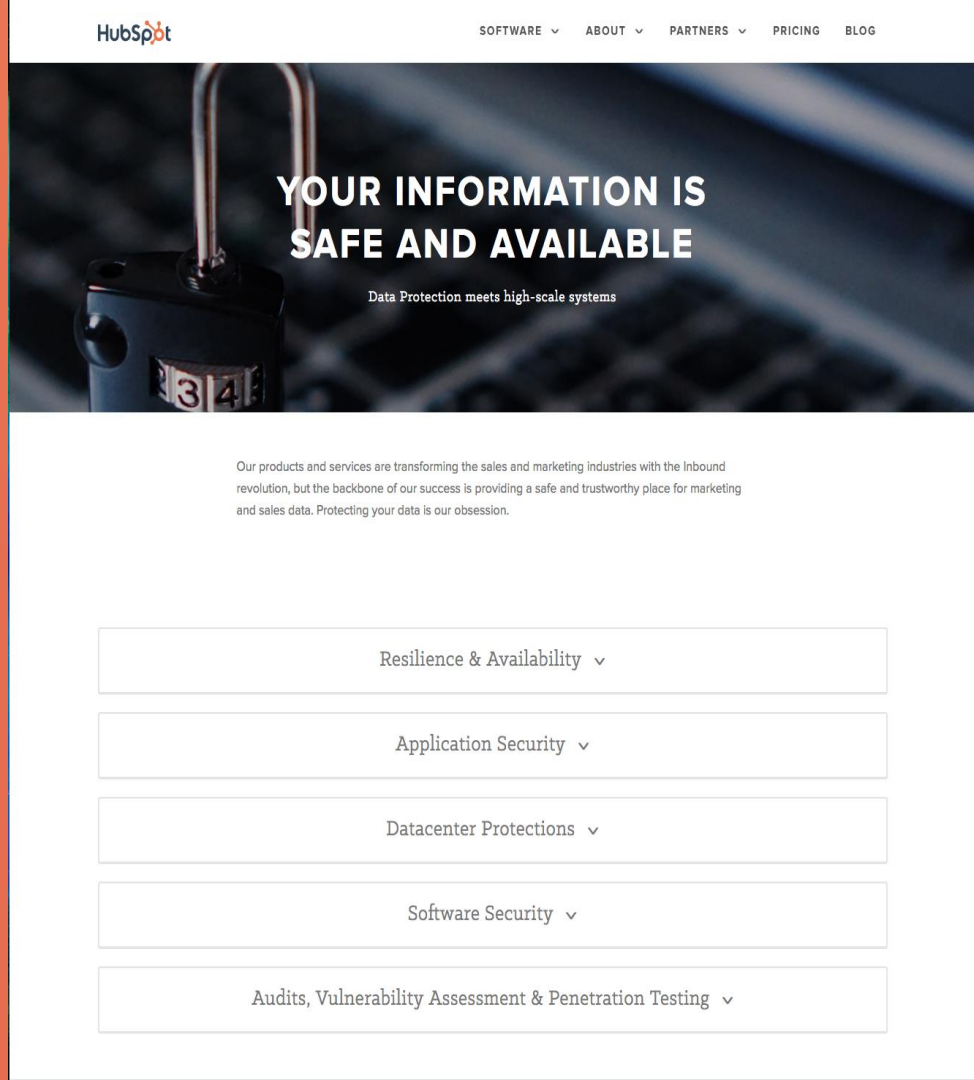
The Procedures and Controls

- Are our Security team informed to ensure they're aware of their obligations under the GDPR and do they have sufficient resources to implement any required changes or new processes?
- Do we have procedures in place to handle requests from data subjects to modify, delete or access their personal data? Do these procedures comply the new rules under the GDPR?
- Do we have security notification procedures in place to ensure we meet our enhanced reporting obligations under the GDPR in case of a data breach in a timely manner?
- Are our staff trained in all areas of EU data privacy to ensure they handle data in a compliant manner?
- Do we review and audit the data we hold on a regular basis?

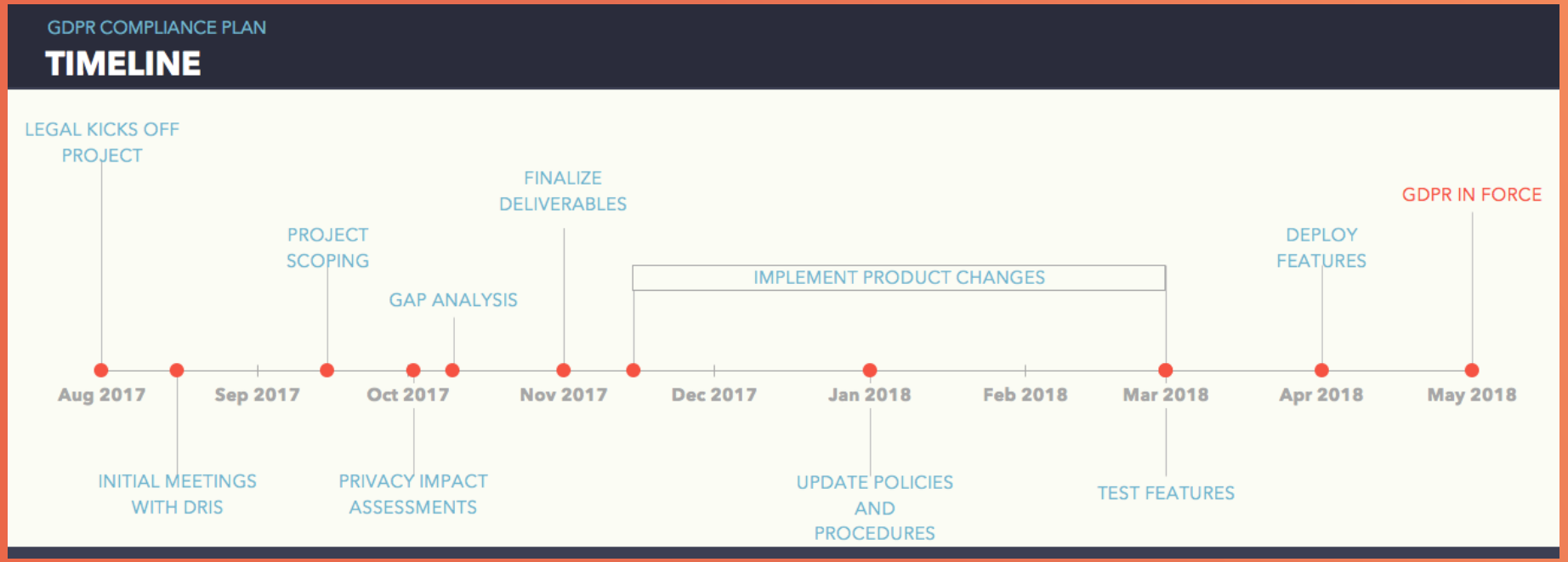
Education and Documentation:

Our Security Best Practices

- hubspot.com/security



Our Timeline



QUESTIONS?

HubSpot
PARTNER DAY 2017

APPENDIX

GDPR: SCOPE

- GDPR expands the territorial and material scope of EU data protection law.
- Applies to both controllers and processors established in the EU.
- Captures controllers and processors outside the EU, who offer goods and services to, or monitor, EU residents.

GDPR: DEFINITIONS

- GDPR broadens the definition of personal data and sensitive data.
- Personal data now expressly includes an identification number, location data, IP address and online identifier.
- Pseudonymisation, where directly identifying data is held separately and securely from processed data to ensure non-attribution, is useful technique.
- Anonymised data is not considered to be personal data.

GDPR: ACCOUNTABILITY

- GDPR requires controllers and processors to be able to demonstrate how they comply with the data protection principles.
- Businesses no longer have to register or notify supervisory authorities of their processing activities.
- Data controllers and processors must implement appropriate technical and organisational measures to show their processing is in accordance with GDPR.
- Records of processing activities must be kept and supplied to supervisory authorities on request, to demonstrate their compliance with the GDPR.

GDPR: CONSENT

- Consent will become more difficult to rely on to legitimise processing.
- Must be verifiable
- GDPR blurs the distinction between consent and explicit consent, as both require some form of clear affirmative action. Silence or pre-ticked boxes will no longer be sufficient to constitute consent.
- GDPR permits data subjects to withdraw their consent at any time.

GDPR: NOTICES

- GDPR provides a list of specific, additional, information that must be provided to data subjects to ensure all processing activities are transparent.
- List includes, in particular, the purpose of collection, the legal basis for the processing, the data retention period or criteria used to determine same.
- Data subjects must also be notified of their right to withdraw consent.

GDPR: ACCESS

- The GDPR requires the provision of specific, additional, information to data subjects when responding to access requests.
- The time period for dealing with requests has been reduced from 40 days to 1 month.
- A data subject access request can only be refused where it is “manifestly unfounded or excessive, in particular because of its repetitive character."

GDPR: PORTABILITY

- GDPR provides data subjects with new rights, including a right to data portability, and a right not to be subject to a decision based on automated processing, including profiling, in certain circumstances.
- It gives data subjects more control by enabling them to object to processing which is based on the legitimate interests of the controller or a third party (including profiling based on that ground).
- Profiling: “any form of automated processing of personal data consisting of the use of personal data to evaluate personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability or behaviour, location or movements"

GDPR: REPORTING

- Controllers have a mandatory obligation to report data breaches to their supervisory authority within 72 hours, unless the breach is unlikely to result in a risk to the rights of data subjects.
- Controllers also have to notify data subjects where the breach is likely to result in a “high risk" to affected data subjects.
- Controllers must keep an internal record of all data breaches.

GDPR: PENALTIES

- GDPR provides supervisory authorities with the power to impose significant fines on controllers and processors for non-compliance.
- Businesses will face fines of up to €20m or 4% of the total worldwide annual turnover of the preceding financial year.
- Fines can be imposed in addition to, or instead of, any corrective measures (such as warnings or reprimands).