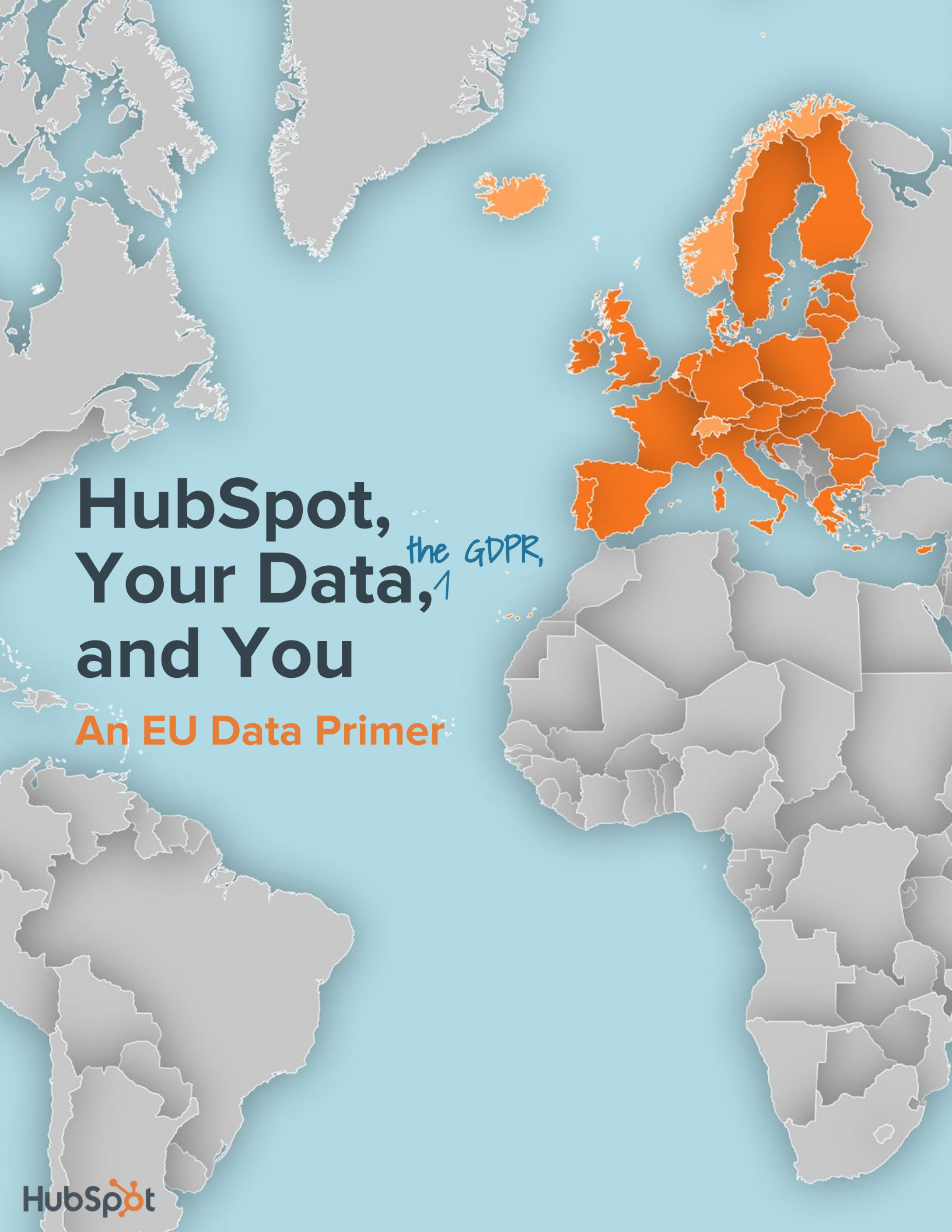

HubSpot, Your Data, and You

the GDPR, 1

An EU Data Primer

HubSpot

HubSpot, Your Data, and You

An EU Data Primer

Last updated on August 4, 2017

You can download the most recent version of this paper and get more information about HubSpot's approach to data privacy at http://legal.hubspot.com/data-privacy.

Data privacy in the European Union, especially in light of the EU's new General Data Protection Law (GDPR), can feel like a confusing question to unpack. At its simplest, it boils down to one thing: trust. The EU and its member states have put legal restrictions in place to ensure that when companies collect data from individuals, they're being honest about why they're taking it, what they're doing with it, where they're keeping it, and who they're sharing it with. When companies do share that data (such as when they rely on a technology vendor to help keep their business running), these laws require that the company ask their vendors for similar promises. All told, these laws establish a protected flow of data from individuals to companies they trust, and then from those companies to the vendors they trust.

A QUICK DISCLAIMER: At the outset, you should know that this paper is neither a magnum opus on EU data privacy nor legal advice for your company to use in complying with EU data privacy laws like the GDPR. Instead, it provides background information to help you better understand how HubSpot has addressed some important legal points. This legal *information* is not the same as legal *advice*, where an attorney applies the law to your specific circumstances, so we insist that you consult an attorney if you'd like advice on your interpretation of this information or its accuracy. In a nutshell, you may not rely on this paper as legal advice, nor as a recommendation of any particular legal understanding.

Table of Contents

A Brief History

To understand where "trust" first came into play, you need to go all the way back to just after the end of the Second World War. In an effort to unify the countries of Europe, a group of states signed a treaty to form the Council of Europe (CoE) in 1949. Soon after, the CoE voted to adopt the European Convention on Human Rights, an international treaty listing out fundamental rights and freedoms to be guaranteed in member states. Number eight on that list included the following commitment, a powerful first step towards the idea of data privacy:

> Everyone has the right to respect for his private and family life, his home and his correspondence.

In 1980, the CoE doubled down on this commitment, coordinating with the Organization for Economic Cooperation and Development (OECD) to draft Treaty No. 108 to regulate the "automatic processing of personal data". It introduced basic principles of data privacy that appear in many of the subsequent laws to address data handling:

- A duty to obtain and process personal data fairly and lawfully
- A duty to store personal data only for specified, legitimate purpose
- A duty to collect the data in an adequate, relevant, and non-excessive manner based on that purpose
- A duty to preserve the data's accuracy, including via updates
- A duty to preserve data that can be tied back to a person for no longer than required for that purpose
- A further restriction on processing of "special categories" of personal data, like race, religious beliefs, or health
- A requirement to maintain "appropriate security measures"
- Additional rights for people to request information on whether their personal data is being stored, and to request updates or deletion of that data

Every EU member state has since ratified the Treaty, making it an important foundation for data protection in the EU.

In 1995, the EU passed the European Data Protection Directive (95/46/EC, the "DPD") to protect an individual's privacy rights and regulate the processing and movement of personal data. The DPD was designed to give substance to the rights established in Treaty 108 and has been the main legal agreement governing data protection and privacy in the EU for the past

twenty years. As a "directive", the DPD worked as a template, laying out certain minimum rules around data privacy that member states were required to enact into law in their countries. The result was a network of European laws that overlapped substantially but varied somewhat from country to country.

The DPD focused on setting standards for entities to follow when collecting and processing personal data from individuals in the EU ("data subjects"). It imposed most of these standards on the entities who collected the data and chose how to use it ("controllers"), but also laid out rules for the vendors who these controllers used to process or store the data ("processors"). These rules covered many familiar data privacy concepts, like obtaining consent from data subjects before using their data, treating sensitive data with extra care, ensuring appropriate security measures, scrutinizing relationships with any vendors who might help a controller process or store data (especially those located outside the EU), and allowing data subjects to control the use of their data. Additionally, the DPD required member states to establish one or more national regulators (known as "data protection authorities" or "supervisory authorities") responsible for monitoring and enforcing the member state's data privacy laws.

With countries outside the EU often not offering the same protections for data, the DPD's drafters chose to focus in particular on the transfer of personal data outside the EU. Article 25 of the DPD introduced a set of geographic restrictions on data transfer, allowing transfers outside the EU only where the European Commission determined that the non-EU "third country" could ensure an "adequate level of protection" (often called an "adequacy finding"). Absent an adequacy finding (there are currently only nine on the list), data controllers looking to transfer data to a third country were forced to rely on one of the few other pre-approved options (like the Model Clauses) or a custom agreement approved by the necessary governmental bodies.

Ensuring Adequacy

One major player was left off the EU's short adequacy list: the United States. This decision was based in large part on the fact that the US has a different approach to regulating data privacy, choosing to regulate specific industries instead of applying blanket rules. As a result, transfers from the EU to the US would only be allowed if a data controller relied on the Model Clauses or if the US chose to enter a policy agreement with the EU guaranteeing adequate levels of protection.

The first major attempt at a policy agreement was the Safe Harbor framework, approved by the U.S. Department of Commerce ("DoC") and European Commission in 2002. US companies would opt into the Safe Harbor program, and were required to certify to the DoC that they were compliant with a number of privacy principles. The principles required participating companies to (1) inform data subjects that their personal data was being collected and how it was being used; (2) provide mechanisms to opt out of data collection and forwarding of data to

third parties; (3) ensure that third party processors had adequate levels of protection; (4) allow data subjects to access their personal data; and (5) make reasonable efforts to prevent loss of information and ensure that data was relevant and used for purpose for which it was collected. US companies complying with these principles and certified under the Safe Harbor program could then permissibly receive data from the EU in compliance with the DPD's adequacy requirements.

Realizing that many other third countries wouldn't make the short list of countries whose laws were found to offer "adequate" protection without further safeguards, the drafters of the DPD also included a provision that the European Commission would have the authority to approve "certain standard contractual clauses" as offering sufficient safeguards to allow transfer to a third country.

Thus far, the Commission has approved three sets of such clauses, which are often referred to as the "Model Clauses". The first two sets were intended for an "EU-controller to Non-EU/EEA-controller" (aka "controller-to-controller") relationship, but the third set covers a "controller-to-processor" relationship – perfect for an automated service provider like an IT or software vendor. Approved in Decision 2010/87/EU, the third set acts as a template agreement between an EU-based controller (the "data exporter") and a US-based processor (the "data importer"). The agreement is structured as a series of twelve clauses that detail the obligations of the processor and controller and rights of the data subjects, with two appendices containing blanks for the importer to detail what data they'll collect, how they'll process it, and what security measures they have in place.

In October 2015, the European Court of Justice (the ECJ) issued a judgment declaring the Safe Harbor framework invalid. Spurred by a suit between Austrian law student Maximillian Schrems and Facebook, the ECJ held that Safe Harbor didn't ensure adequacy for transfers to the US because of weaknesses in the remedies offered to data subjects and a failure to fully address potential US government surveillance. Since custom solutions for ensuring adequacy often take years to implement, businesses raced to implement the Model Clauses for data transfers formerly covered by their participation in the Safe Harbor program.

Fortunately, the EU and US quickly realized the necessity of a replacement, referred to by many as a "Safe Harbor 2.0", and began discussions to implement a new framework. In July 2016, they published the final version of the new scheme, which they called the EU-U.S. Privacy Shield framework, allowing US businesses to self-certify starting on August 1, 2016. The Privacy Shield built on the the work of Safe Harbor, with a certification process friendly to small and medium businesses and a "blanket" applicability to data transfers from all of a certified US entity's customers in the EU. To address the flaws that the *Schrems* case identified in Safe Harbor, however, the Privacy Shield framework also added new commitments to data subject rights, protection during onward transfer to sub-processors, and cooperation between the EU and US on alleged infringements and government surveillance.

The GDPR

In the two decades since the DPD was first passed, the internet has changed quite a bit. From the ubiquity of US software-as-a-service providers like Google, Dropbox, and Microsoft to the growth of the "internet of things", data is being used and shared in ways unfathomable to lawmakers back in 1995 when many lacked home internet and e-commerce was still an unproven concept.

Beyond those changes to the internet that rendered the DPD hard to apply, the EU had also realized a fundamental limitation of the "template"-style directive model—despite the DPD's stated goal to harmonize EU data privacy laws, the flexibility afforded to each country when implementing the DPD's requirements had resulted in rules that varied widely in stringency between countries.

EU lawmakers spent years developing a replacement to improve on the DPD's approach, finally implementing the General Data Protection Regulation (GDPR) in May 2016. The GDPR, set to apply starting in May 2018, was structured as a regulation instead of a directive, meaning that it will apply directly to each EU member state without requiring them to amend their laws. The regulation builds on many of the DPD's requirements for data privacy and security, but includes several new provisions to bolster the rights of data subjects and add harsher penalties for violations.

Some of the GDPR's new principles have gotten quite a bit of press. While the DPD governed entities within the EU, the GDPR will also include non-EU businesses who market their products to people in the EU or who monitor the behavior of people in the EU. The GDPR steps up the standard for disclosures when obtaining consent, requiring that consent be "freely given, specific, informed and unambiguous," with controllers using "clear and plain" legal language that is "clearly distinguishable from other matters". The regulation also builds in two new rights for data subjects: a "right to be forgotten" that requires controllers to alert downstream recipients of deletion requests and a "right to data portability" that allows data subjects to demand a copy of their data in a common format. Finally, there are several new principles for entities who develop software and systems that handle personal data, including a requirement to build in data privacy "by design" when developing new systems and an obligation to perform a data privacy impact assessment when processing using "new technologies" or in risky ways.

On the security side, the GDPR will require many businesses to have a Data Privacy Officer (DPO) to help oversee their compliance efforts, an especially helpful function in light of GDPR's new requirement that controllers notify their country's supervisory authority of a personal data breach within 72 hours of learning of it. While the GDPR currently preserves the DPD's approved methods for ensuring "adequacy" when transferring personal data to third countries

(including the Privacy Shield and the Model Clauses), DPOs will also be helpful in overseeing a controller's relationships with vendors who process and store personal data, helping to review vendors' security practices and inform vendors of data subject requests. One particular item in the GDPR should serve to make the lives of these DPOs easier: the GDPR's new "one stop shop" provision, under which organizations with offices in multiple EU countries will have a "lead supervisory authority" to act as a central point of enforcement so they don't struggle with inconsistent directions from multiple supervisory authorities.

The importance of the GDPR's new provisions is underscored by the new penalties it imposes for violations. Depending on the type of violation in question, controllers and processors who mishandle personal data or otherwise violate data subjects' rights could incur fines of up to €20 million or 4% of their global annual revenue (whichever is greater).

HubSpot's Approach to the Law

As HubSpot began to attract a larger international audience back in 2012, we made the decision to become Safe Harbor certified. We partnered with TRUSTe, a leading global data privacy management company who certified our privacy practices for compliance with the EU Safe Harbor Framework. For German customers who sought an additional level of assurance to comply with the German Federal Data Protection Act ("BDSG"), we also offered a Data Processing Annex ("DPA") that referenced certain requirements of German law, including certain protections for intra-EU data transfers from German customers to HubSpot's Ireland office.

While Safe Harbor was being challenged in court, HubSpot began to investigate alternatives as our prospective customers started asking about other options. Of the available options, we settled on the Model Clauses as the best bet, offering increased contractual protections for our customers and a relatively quick timeline to implement compared to many alternatives, some of which could take years. Once the new Privacy Shield program was announced, we also made the decision to self-certify under that framework.

Today, HubSpot maintains a Privacy Shield certification with the U.S. Department of Commerce as one way to ensure that adequate safeguards are in place when transferring personal data from the EU to the US. We have incorporated information about our Privacy Shield certification into both our Customer Terms of Service (in the 'EU/EEA Data Processing' section) and our Privacy Policy.

As we approach May 2018, HubSpot is also focused on GDPR compliance efforts. During this implementation period for the regulation, we are evaluating new requirements and restrictions imposed by the GDPR and will take any action necessary to ensure that we handle customer data in compliance with applicable law by the 2018 deadline. We will be providing updates in the time leading up to May 2018 regarding steps we will be taking to ensure that both we and

our product are compliant with the GDPR in advance of the deadline, and recommend that those interested keep an eye on our Data Privacy homepage for updates. We will also be updating our legal documentation before the deadline to reflect any changes to our product and to ensure that, as a processor of our customers' personal data, we meet the requirements of processors under the regulation.

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), seeking their own legal advice to ensure that their business practices comply with the GDPR.

HubSpot's Approach to Security

Given the intricacies of EU data privacy laws, customers often ask thoughtful questions about facets of our product and our security program. Using this understanding of HubSpot's technology, customers can work with their own attorneys to ensure compliance with the laws that apply to them.

Cookies

In 2002, the EU passed the Privacy and Electronic Communications Directive (2002/58/EC, commonly referred to as the "ePrivacy Directive"). The ePrivacy Directive expands on the Data Privacy Directive, focusing on the protection of privacy in electronic communications, such as traffic data and unsolicited emails. Specifically, the ePrivacy Directive establishes an opt-in regime, where prior consent by the recipient is required before sending emails. The initial ePrivacy Directive was amended in 2009 (2009/136/EC, commonly referred to as the "Cookie Directive") to require disclosure and consent for permissible use of cookies.

HubSpot uses cookies to enhance visitors and users experience with the platform. We disclose all cookies in use by the platform, and you can find that information on the HubSpot knowledge base. In general, HubSpot uses cookies in order to provide users with a secure experience when logged into their portal, and to help measure site visitors engagement with content posted to Hubspot portals.

With regard to site visitors, the HubSpot platform uses cookies to help you understand how your website visitors and leads engage with the content that you produce. A cookie is a small file that is left behind on the computer of visitors to websites. When a visitor arrives at your site, it leaves behind a cookie on your visitors' computers that helps HubSpot uniquely identify them. Cookies are also used to help enable features like smart content, in which visitors see tailored content depending on their past visits.

The HubSpot platform uses these cookies to allow you to know what parts of your site a visitor spent time interacting with or reading. If a visitor voluntarily chooses to provide their contact information, the cookie in that browser is associated with the newly created contact record. Browsing history information is available to you in your portal as part of the lead profile. Cookies cannot be used by themselves to identity a person who has not chosen to provide his or her contact information. Only when site visitors voluntarily provide their contact information can subsequent visits be tied to a information about a person.

Site visitors value transparency on the part of the companies whose sites they visit. To help enable that transparency, the HubSpot platform gives you the option of enabling privacy notices on your sites. For more information about privacy policy notifications, please see our Knowledge article about privacy policy popups.

Email Features

HubSpot's email capabilities include several features that help improve your sales and marketing teams' efficiency, and give you the power to reduce unwanted communication to your recipients and prospective leads.

The HubSpot platform gives you the ability to configure your portal in a way that ensures your contacts are interested in the content you make available. The double opt-in feature increases the assurance you have that your contacts are right for your message. You can read more about enabling double opt-in in HubSpot's Double Opt-in Knowledge article. With a double opt-in, contacts get the ability to reaffirm their interest in your content. New contacts initially identify their interest by providing their contact information on your landing pages. Before receiving email from you, contacts also must confirm that they want to receive that email. When double opt-in is enabled on your portal, you can confirm that your audience is interested in your message as you are in them.

The HubSpot products also let you understand and make decisions based on the degree to which your recipients open and read your email. You can read about how HubSpot used information about its subscribers' engagement to remove hundreds of thousands of blog subscribers from its email marketing on HubSpot's Graymail blog post.

In order to provide you information about your email recipients' level of engagement, the HubSpot products use a feature called a "tracking pixel". This feature uses image resources in order to identify when a recipient opens an email you send through one of the HubSpot products. When an email is sent through the HubSpot marketing or sales products, an image tag for a tiny image is included in the email body. When a recipient opens the message and if the recipient's email client is configured to do so, the email client will make a request to the HubSpot platform for the image, which is translated into the email open rates available to you in your portal. These pixel requests do not include personally identifiable information and are obfuscated by a long, randomized string.

Data Hosting

The HubSpot platform is hosted in trusted third-party data center providers in the US, and the data stored by HubSpot is stored in the US. HubSpot partners with the world's leading data center providers in order to provide our services to you. Currently, the primary HubSpot infrastructure is hosted with Amazon Web Services in the US-East-1 region. Amazon Web Services maintains ISO 27001, SOC 2 Type II, and several other certifications to demonstrate the rigor of their hosting and infrastructure management program. Information about AWS certifications is available on the AWS Security Compliance site.

Security Program

As a part of our responsibility to keep your data safe, HubSpot focuses on providing transparency into how we help protect our customers' data. Information about our security program is published on HubSpot's security site and in our Security & Risk Management Overview, available in your portal under Settings > Account & Billing > Document Center.

Overall, the HubSpot security program includes advanced threat and attack detection and prevention, 24x7 monitoring and alerting, and sophisticated bug discovery capabilities. The platform is built with multiple levels of redundancy and failover, and lives in data centers that are renowned for their resiliency. The HubSpot experience takes advantage of state of the art content distribution, meaning that your and your visitors' browsing experiences are fast regardless of your location.

Amending Data & Other Privacy Requests

Everyone who provides his or her contact information to HubSpot has the right to request that they not be contacted or that their information be corrected. Our privacy team can be reached at privacy@hubspot.com and is dedicated to ensuring that HubSpot continues to be a positive influence on the reputation of content marketing and sales communities.

Privacy requests sent to HubSpot are automatically forwarded to an on-call specialist. Each request is tracked through its lifecycle from receipt to closure, and additional resources are brought in, depending on the specifics of a request. Information about HubSpot's approach is also available in our Privacy Policy.

Looking Ahead

Data privacy in the EU has been an ever-evolving field, and in the last few years those evolutions have come at a rapid pace. HubSpot keeps a close watch for any updates in the data privacy sphere, relying on close relationships with regional law firms and data security

service vendors like TRUSTe to ensure that we're up to date when regulations are enacted or struck down. The members of HubSpot's Legal team also share updates with the broader company when changes to the law impact us or our customers.

Currently, we believe the best available approach is to offer our EU/EEA customers additional terms in our Customer Terms of Service that reference our Privacy Shield certification. Just as we transitioned from reliance on Safe Harbor to a reliance on Privacy Shield, however, we will evaluate any new options to establish adequacy for transferring data outside the EU. In the months leading up to May 2018, we will also be incorporating GDPR compliance efforts into both our day-to-day operations and our product, and will post updates on those efforts to http://legal.hubspot.com/data-privacy.

One question we're sometimes asked is whether we have any plans to open a data center in the EU. This question is prompted by the fact that, as mentioned in the Data Hosting section above, we currently rely on AWS's US-based hosting service for our data storage. We are currently looking into the feasibility of an EU-hosted offering and, while we cannot provide any specific timeline, we will keep you updated as we learn more about our options surrounding EU data storage.

As the state of data privacy laws, security best practices, and international software platforms continues to evolve, we will stay up-to-date on all new developments so we can respond in a way that keeps customer data safe and ensures our compliance with applicable laws. Where new legislation is due to come into effect, we work with outside counsel and other resources to ensure that our plan of attack covers all the changes we need to make. At the end of the day our goal here at HubSpot is to make sure we preserve something very important to us: our customers' trust.

Additional Resources

If you've still got questions, we recommend the following resources to dig in deeper:

- General
  - Data Protection, European Commission
  - Handbook on European Data Protection Law, EU Agency for Fundamental Rights (2014)

- Data Transfers Outside EU
  - Model Contracts for the transfer of personal data to third countries, European Union (2010)
  - Updated EU Model Clauses, WilmerHale (2010)
  - The Demise of the US-EU Safe Harbor, Hunton & Williams (2015)
  - Privacy Shield Program Overview, U.S. Department of Commerce (2016)
  - GDPR - Cross-border data transfers, Loyens Loeff (2017)

- EU GDPR
  - Regulation (EU) 2016/679 [GDPR], European Union (2016)
  - A Brief History of the GDPR, IAPP (2016)
  - General Data Protection Regulation Guide, Jones Day (2017)
  - A Guide to the General Data Protection Regulation, DLA Piper (2016)
  - Unlocking the EU General Data Protection Regulation, White & Case (2016)
  - GDPR Compliance Update: Which Government Authorities Have Issued Official GDPR Guidance?, Proskauer (2017)

- Cookies & IP Addresses
  - IP Addresses as Personal Data, Orrick (2016)
  - EU regulators welcome stricter rules on cookies and direct marketing, White & Case (2017)