FREQUENTLY ASKED QUESTIONS

TrustArc's "Marketing Under the GDPR" Webinar: Your Questions Answered

A Summary of Key Questions from Webinar Participants, Together with Responses Prepared by Members of the TrustArc Team of Privacy Experts

Overview

On May 25, 2018, the European Union's General Data Protection Regulation (GDPR) will take effect, ushering in the most consequential changes to EU data protection law--and companies' internal data governance practices--in more than two decades. Because of the law's extraterritorial reach, it can apply to companies located anywhere in the world that are collecting or processing EU-originating personal data.

Many core business competencies will be affected by this sweeping new law, and prominent amongst them are organizations' marketing departments and activities.

On January 17, 2018, TrustArc hosted a webinar entitled "Marketing Under the GDPR" to discuss the impact of the GDPR on marketing activities. What follows is a summary of many of the questions submitted by participants during and after the webinar, along with answers prepared by members of TrustArc's team of privacy experts.

In addition to this comprehensive set of FAQs, Team TrustArc is available to help you further review your GDPR readiness and offer our award-winning technology solutions for compliance. To find out more information on options that meet your business needs, visit https://www.trustarc.com or call 1-888-878-7830.

Sections

1. This memorandum is intended as a general overview of the subject and cannot be regarded as legal advice.

Section A. Business-To-Business (B2B) Applicability

Is a business email address considered personal data in the EU?

Yes, business contact information is considered personal data (PD) under the GDPR's Art. 4 definition for that term, which is "any information relating to an identified or identifiable natural person ('data subject') ..." So, "jane.smith@company.com" is personal data, but "sales@company.com" is not, because an identifiable individual exists for the former but not the latter.

Moreover, also included within the scope of "personal data" are technical identifiers, location data, IP address, and other information that directly or indirectly can identify a distinct person, regardless of context (B2B, business-to-consumer (B2C), etc.).

And so, if collecting or using such personal information for marketing activities, an organization must have a legal processing basis for doing so per GDPR Art. 6.

Does GDPR apply if we share EU personal data with our affiliates or partners?

GDPR applies whether an organization shares its B2B/B2C marketing lists with affiliates or partners; uses a third-party marketing list; or engages a vendor to carry out direct marketing on its behalf.

We are a white label email hosting company. We provide email services to companies, and THOSE companies have end users. Our clients are the ones that collect data on their own customers. How does the GDPR affect us?

It of course always depends on the specifics of any given situation, and you should consult your organization's counsel, but if you are processing EU personal data (i.e., performing some automated or manual operation on a personal data set per Art. 4's definition), even in solely the capacity as a data processor, you will have to comply with the GDPR (including, e.g., contract updates per Art. 28, keeping detailed records of processing per Art. 30, notifying controllers of data breaches per Art. 33, and complying with cross-border data transfer requirements per Ch. 5).

Section B. Consent and Marketing Under the GDPR

Do I need to have consent to collect EU personal data (PD) for marketing?

The GDPR requires that personal data be "processed lawfully, fairly and in a transparent manner." The law further sets forth six legal bases for processing, one of which is a data subject's consent to processing PD for "one or more specific purposes" per Art. 6.

As described more fully below, it is possible per Recital 47 that processing PD for direct marketing purposes may also be legally justified using a "legitimate interests" balancing test, but exactly how this will be understood and interpreted by regulators remains to be seen.

For companies seeking to rely on consent as a legal basis for processing, per Art. 4 consent must be a "freely given, specific, informed and unambiguous" indication of a data subject's agreement to processing, and thus provided by a clear affirmative action (R.32)--not silence, pre-checked boxes, or bundled together with other terms and conditions, i.e., it must stand apart from other terms and conditions, and be granular as to the specific data uses for which consent is being requested.

1. This memorandum is intended as a general overview of the subject and cannot be regarded as legal advice.

By having this statement before a subject enters into a sweepstakes online, for example, and no opt-in box, is that enough for informed consent? "By entering, you understand that you are agreeing to receive information from XYZ Company and its sponsors," or "by submitting this form, you agree to…"

This is unlikely to qualify as meaningful, demonstrable consent for GDPR purposes. Formerly used "opt-out" approaches generally will not meet the new standard because they are not "unambiguous" indications of an individual's affirmative agreement to specific processing uses for which consent is being requested.

A good rule of thumb for organizations is to ask whether they can supply a record of the time, date, and intake mechanism for instances when a data subject's specific consent was captured. If they cannot, and thus cannot demonstrate consent, they may need to re-obtain GDPR-compliant consent if they wish to rely on consent for processing.

Can a company give consent on behalf of its employees to send them marketing communications using their work email address/phone numbers?

Third-party consent is generally not permissible under the GDPR--individuals must consent for themselves to the processing of their own personal data. Moreover, the provision of consent in an employer-employee context is problematic, given the "freely given" nature required for consent.

Can my company capture consent in exchange for content? For example, collecting email address to download a white paper or register for a webinar?

Yes, but organizations must clearly state at the time of information collection what the specific uses of the information will be--and any non-disclosed purposes will likely not be deemed consented to if challenged.

For instance, an organization could not use email addresses obtained solely for contest entry purposes to then market to the individual or share that information with partners, unless the user also was asked and specifically and actively agreed to the organization using their personal data to do so. In this way, consent must be granular as to the intended uses.

What is "stale" consent and re-permissioning for legacy contacts?

"Stale" consent is consent that was previously obtained (e.g., under the standards of the existing Data Protection Directive and its national implementing legislation) but which does not meet the GDPR's new standards for consent. For instance, consent previously obtained through "opt-out" methods or the use of pre-ticked boxes will generally not satisfy the clear, affirmative action requirement, and thus would not serve as consent under the GDPR.

Organizations should thus evaluate their previous and existing methods of obtaining informed consent, and for any instances that do not satisfy GDPR standards, seek to obtain GDPR-compliant consent from those legacy individuals--or else no longer use the earlier, acquired personal data. This requesting of consent from individuals whose previously obtained consent did not meet GDPR standards is what is referred to as a "re-permissioning" or "re-engagement" campaign.

1. This memorandum is intended as a general overview of the subject and cannot be regarded as legal advice.

Can we reach out to individuals who have previously unsubscribed from our marketing communications to obtain their consent under GDPR standards?

No, if individuals have unsubscribed, opted out, or otherwise indicated their desire that your organization stop using their personal information, your organization may not nonetheless contact them to seek their consent to marketing. Art. 21(3) further states: "Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes."

Even under the outgoing EU Data Protection Directive and related national legislation, the U.K. ICO last year fined multiple companies that sent emails to individuals who had already opted-out of marketing emails--asking those same individuals to update their marketing preferences, including whether they wanted to opt-in to receiving future marketing messages. As the ICO stated: "Sending emails to determine whether people want to receive marketing without the right consent is still marketing and it is against the law...businesses must understand they can't break one law to get ready for another."

What if we received a list from a partner and we market based on their list? If we're unaware of any notice or opt-in, can we still send to individuals on that list?

Organizations should evaluate the methods through which they obtained all EU personal data. If a company markets to individuals but is not able to demonstrate when and how consent was obtained (if consent was the legal basis for processing), or the consent was given for other specific parties to direct market, then the new marketer may be subject to regulatory questioning or even enforcement actions.

If an organization wishes to use bought-in lists for texts, emails or recorded calls, it should be prepared to provide proof of opt-in consent that specifically names or clearly describes the organization, and the fact that that organization will market to the individual.

If we do a partner webcast and they host a webcast sponsored by us, can we use those names? How might this work, as it seems there is no longer any benefit to teaming up with partners.

Organizations may continue to partner with others, but they will first each need to have clarity--based on the facts of the given situation--as to their status as data controllers, data processors, or joint controllers.

Provided individuals are made specifically aware of all parties collecting and using their personal information, and this and the proposed uses of the personal data are actively agreed to by the individual, data obtained through partnerships can be validly used.

So, can I share my event participants lists (e.g., full name and company name) with other event participants?

An organization can share lists, provided it has made clear that the personal data the individual provides will be shared with others--specifically naming them or providing clear descriptions of them--for their own marketing purposes. If relying on consent to do so, the organization should obtain granular, affirmative consent to this from the individual and keep a record of this consent, as partners and buyers will likely demand proof of the data subject's opt-in to having their registration information shared with others.

1. This memorandum is intended as a general overview of the subject and cannot be regarded as legal advice.

Does a clear and concise privacy notice on a form comply with GDPR to collect personal data (email campaigns aside)?

While having such a privacy notice may satisfy the GDPR's heightened transparency requirements (including those set forth in Art. 12 and elsewhere), a notice alone will not satisfy the consent standard for collecting or processing EU personal data, as evidence of unbundled, affirmative action indicating agreement to processing on the part of the end user would be lacking.

Do I need a "double opt-in" for email collection?

The GDPR does not specifically reference a double opt-in, but organizations that do so as a best practice can feel that much more confident from a risk management perspective that they have obtained affirmative express consent to specific marketing purposes in an unbundled manner.

Section C. Vendors

What process do we need to follow to have vendors confirm they have consent to contact individuals?

This may vary for each company, and so check with your organization's counsel, but it is advisable to have strong contractual provisions in place--with any company obtaining consent or sending messages on your organization's behalf--obligating the provision of notice and capturing of informed consent, as well as the right to audit or to be provided access to the records of consent which list your organization as a possible recipient for specifically described purposes.

What are the key questions that a marketer needs to ask their email service provider (ESP) to know the ESP is actually ready and can help the marketer be GDPR-ready?

Organizations should be ensuring that their email service provider is aware of their obligations under Article 28 of the GDPR. They should be asking their ESP if they are able to assist in demonstrating compliance with the GDPR (Article 28 (3-f). A comprehensive vendor assessment as well as a data protection agreement which incorporates standard contractual clauses are also recommended.

Section D. ePrivacy Directive, Regulation, and Changes to Come

What is the ePrivacy Directive ("EU Cookie Law") and why is it being replaced?

Currently, the EU operates under the ePrivacy Directive (ePD) and its national implementing laws, such as the PECRs in the U.K. The ePD safeguards the confidentiality of electronic communications in the EU, including treatment of traffic data, spam, and tracking technologies across Internet-connected devices. As a directive rather than a regulation, the 28 EU member states have latitude in how to interpret it and what is required for compliance locally, leading to difficulties for multinational companies wishing to operate uniformly across the EU.

This has led to the desire to update the law, in the form of a draft ePrivacy Regulation (ePR) that would serve as a new top-down pan-EU law. The ePR is still going through the legislative process in the EU. TrustArc recently published a client advisory on the ePR draft, a download of which is available here.

1. This memorandum is intended as a general overview of the subject and cannot be regarded as legal advice.

Will there be changes to marketing practices as a result of an update to the current ePrivacy Directive?

As noted, the draft ePrivacy Regulation is still being debated and updated, and so at present it is not in a finalized form, but if and when the ePR takes effect, it will likely have a broad impact on several sectors. For instance, the current draft would extend its rules to "over-the-top" communications and messaging services (e.g., Skype, WhatsApp, FB Messenger, Slack); effectively apply the GDPR's level of consent as a requirement for publishers/apps/websites that wish to store tracking technologies on end users' devices--or, migrate "consent" to users' needing to affirmatively change their browser/device settings; impact metadata uses; apply the GDPR's fine structure; and trigger other changes to the "ad tech" and interest-based advertising space. TrustArc continues to closely watch the ePrivacy debates and eventual final legislation.

Section E. Different Forms of Marketing

Can I continue to engage in direct telephone call marketing?

Yes, but you must do so in compliance with legally obtained contact lists, verified against local "do not call" registries, and pursuant to local law. For instance, in the U.K., the Privacy Electronic Communications Regulations (PECR) presently give people specific privacy rights in relation to electronic communications such as marketing calls, emails, texts and faxes, as well as cookies/tracking technologies, and other security provisions.

As noted above, draft legislation is currently moving through the EU legislative process that will update the ePrivacy Directive into a Regulation, likely impacting direct marketing rules across channels vis-a-vis how they exist under current national legislation today.

If I get consent in a phone call, do I have to record the call?

Check with your organization's counsel regarding local laws and marketing practices, but, at a minimum, best practices dictate having formal permission to contact an individual in the first place, and then announcing at the beginning of the call that the call is being recorded, and then specifically explaining the purpose for which consent is being requested.

Can I "cold call" a potential customer? Would it be safe to say that you can carry on, as you cannot identify the person through the number, but need to request the consent after explaining the reason behind the call?

Such a practice is likely to run afoul of marketing regulations and it would be advisable to have a clear basis for contacting any potential customers.

Section F. TrustArc

Does TrustArc have solutions to any of these new compliance hurdles?

Absolutely. TrustArc has best-in-class solutions developed over our 20 years in the privacy space. Please check out our Cookie Consent Manager, Data Flow Manager, Individual Rights Manager, Ads Compliance Manager, GDPR DPIA/PIA Solutions, and our international data transfer certification offerings, for example. Each may be used in furtherance of GDPR compliance.

1. This memorandum is intended as a general overview of the subject and cannot be regarded as legal advice.

When will TrustArc issue a GDPR certification program?

GDPR certifications will not formally be allowed until the European Commission officially sets forth rules and criteria for them. TrustArc is closely following these developments. In the meantime, TrustArc offers GDPR Strategic Priorities Assessments, DPIA/PIA Consulting, Privacy Shield Verifications and Privacy Risk Assessments.

Do you have any GDPR compliance checklist/roadmap consulting services for small start-ups?

TrustArc's GDPR Priorities Assessment and related GDPR/Privacy offerings are suitable for companies ranging in size and maturity from start-ups to Fortune 100 companies.

Section G. Legitimate Interests

Much discussion has to do with using consent as the legal basis for marketing, and much of the literature tends to assume that consent will always, or almost always, be required. Where, if ever, can marketers rely upon legitimate interests as pointed to in GDPR Recital 47? Do you expect the ePrivacy Regulation to effectively shut that door?

Recital 47 of the GDPR states, *"the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."* This may be where obtaining consent is not possible or not preferred. That said, organizations will still need to show there is a balance of interests – their own and those of the person receiving the marketing. If a controller in good faith believes individuals have a reasonable expectation that their data will be processed, this may help them make a case for relying on legitimate interest. Additionally, there may be a relevant and appropriate relationship, for example, if the data subject is an existing client.

The draft ePrivacy Regulation relies on the data subject's consent more than the GDPR, which provides a wider number of alternative solutions, including the legitimate interest. On the contrary, the latest draft of the ePR states:

"The provider of the electronic communications service may process electronic communications data solely for the provision of an explicitly requested service, for purely individual usage, only for the duration necessary for that purpose and without the consent of all users only where such requested processing does not adversely affect the fundamental rights and interests of another user or users."

This position seems confirmed also in relation to communications for direct marketing purposes whose provision of the ePrivacy Regulation refers to the need of a prior consent, only providing for the "soft spam exemption" and without mentioning the possibility of relying on legitimate interest, which is expressly provided by the GDPR.

Recital 47 tells us that processing of personal data for direct marketing may be regarded as carried out for a legitimate interest. So, should this not be considered as a lawful basis rather than consent?

The GDPR does provide for legitimate interest as a legal basis for using personal data without obtaining consent. A legitimate interest provision was also included in the previous EU Data Protection Directive 95/46/EC. However, the GDPR now includes an explicit mention of direct marketing as a legitimate interest (Recital 47), which has led many organizations to believe they will not have to ask data subjects for permission to use their personal data. A legitimate interest is a clearly articulated benefit to a single company, or to society as a whole, that can be derived from processing personal data in a lawful way. However, the Article 29 Working Party has already made it clear that merely having a legitimate interest does not entitle one to use personal data. The objective of the "legitimate interest" provision is to give controllers "necessary flexibility for data controllers for situations where there is no

1. This memorandum is intended as a general overview of the subject and cannot be regarded as legal advice.

interest" provision is to give controllers "necessary flexibility for data controllers for situations where there is no undue impact on data subjects". The Article 29 Working Party cautioned that it is not to be used "on the basis that it is less constraining than the other grounds".

Will "soft opt-in" continue to exist under the GDPR?

Under existing law, consent is not required if an organization is sending marketing messages about similar products or services to current customers, as long as: (1) they have the opportunity to opt-out when the org obtains their contact information; and (2) they have the opportunity to opt-out when the org sends them any future marketing messages. This exception for existing customers is referred to as the "soft opt-in."

As this processing is actually not based on consent but rather legitimate interests for its legal basis, it is likely that soft opt-in will still be allowed under the GDPR, but organizations should be cautioned that more guidance is needed in this area before definitive conclusions can be made.

Section H. Enforcement

Do you have any thoughts on the likelihood of a U.S. federal court enforcing this extraterritorial EU law against a U.S. company - or allowing a suit by an EU data subject or EU data authority against a U.S. company that does not operate in the EU but does process EU personal data?

We can't opine as to the jurisdictional issues that could arise in such a situation within U.S. courts, but it is clear that the law has an extraterritorial reach and Art. 82 states that any person who has suffered material or non-material damage as a result of a GDPR violation "shall have the right to receive compensation from the controller or processor for the damage suffered."

Do you feel there are target companies that regulators will focus on initially? Will there be an enforcement grace period?

Regulators have stated that companies should be prepared for enforcement on "day one" (May 25, 2018), and that the preceding two years are the grace period. Moreover, companies of all sizes and sectors that collect or process EU personal data are subject to the law, meaning that small, medium, and enterprise-sized companies in all verticals should be ready to demonstrate their compliance.

Section I. Global Interoperability

Do you anticipate that other areas of the world will adopt/enact legislation similar to GDPR? In other words, if I don't believe GDPR impacts me directly today how soon will it?

Indeed, in response to massive data breaches and rising consumer expectations, jurisdictions across the globe are creating or modifying their data protection laws to require more data subject rights, enhanced security measures, contract updates, and greater organizational accountability. It is possible, for instance, that this year Japan and/or South Korea will receive adequacy determinations from the EU, finding that those countries' data privacy laws provide essentially equivalent safeguards as the EU, thereby allowing for cross-border data exports to those countries as though they were in the EU.

1. This memorandum is intended as a general overview of the subject and cannot be regarded as legal advice.

In this regard, organizations' work towards GDPR or compliance with other frameworks and national laws may be complementary and used in service of the other. For this reason, frameworks such as the APEC Cross Border Privacy Rules (CBPR), and soon the Privacy Recognition for Processors (PRP), will increase in salience and utility to companies globally.

Are there any jurisdictional or other issues with accessing EU list serves and contacts databases from the U.S.?

As described in GDPR Ch. 5, companies in the U.S. and elsewhere outside the EU must have a legal transfer mechanism for receiving or accessing EU personal data. Accordingly, organizations must evaluate the methods they use for receiving/transferring/importing EU personal data and document their transfer basis.

Many U.S. companies self-certify to the EU-U.S. Privacy Shield Framework for their legal mechanism--with TRUSTe having formally verified hundreds of them. More information is available here: https://www.trustarc.com/products/privacy-shield/.

Section J. GDPR Miscellaneous

How do some of these GDPR requirements apply to capturing details in order to fulfill an order (e.g., order details, payments, shipping etc., as opposed to marketing)?

Check with your organization's counsel, but in some cases, this may qualify as necessary for the performance of a contract that the data subject requests, in keeping with the legal processing basis set forth in GDPR Art. 6(1)(c).

Service emails - can we still add a small (max. 20%) marketing message? i.e., product recommendations?

Check with your organization's counsel, but in general regulators tend to adopt the view that marketing messages embedded within transactional/customer service emails are in fact marketing communications, so be wary.

What about photos in the marketing context?

Depending on their use, photographs may constitute "personal data" under the GDPR if they directly or indirectly relate to an identifiable individual.

Subject access requests (SARs) are now required to be free? We can't charge a fee?

GDPR Arts. 12 and 15 state that data subjects have the right to access certain information that data controllers hold about them, and that this must be free of charge unless the request is "manifestly unfounded or excessive," in which case a reasonable fee may be charged taking into account the administrative costs of providing the information.

1. This memorandum is intended as a general overview of the subject and cannot be regarded as legal advice.

Section K. Lead Generation and Business Cards

The exchange of business cards is not a consent to receive direct marketing, but it can be still used to exchange emails (person to person) and in the contents of that email can be a request for the person to consent (or not) to receive future direct marketing. Is this correct?

At the moment, there is still no clear guidance on this specific subject. The worst-case scenario, if a strict interpretation of the GDPR is used, would mean the handing over of a business card could not be considered sufficient as 'provable consent'. In other words, following this interpretation, you should have proof that every person in your database has given consent to receive the communications from you. The reality which (if the European Commission actually confirms the strict interpretation of the GDPR) should then be accepted, is that exchanging a business card at an event and adding the information to your marketing database is not going to be sufficient. Instead, marketers are encouraged, e.g., to set up a form fill on an iPad or other device at the exhibition and use this as a way to capture opt-in data from attendees.

Can you provide greater clarity on attendee lists? Are they ok to use or not? Will trade show vendors need to change how they share attendee info? Right now, they typically email lists to us.

Attendee lists or delegate lists would only be okay to use of the entity collecting the data has obtained the consent of the data subject(s) as well as informed them how their data will be used and shared. Personal data is defined as any information related to a person or 'data subject' that can be used to directly or indirectly identify the individual. It can be anything from a name, email address, photo, or computer IP address to more detailed information on medical conditions, dietary requirements and social media posts, even photos of attendee badges displaying individual QR codes fall into the category. Event organizers need to provide details around how they will store, process and/or share any data obtained at tradeshows.

How does GDPR impact the LinkedIn contact? Can we approach prospects via connecting in LinkedIn and then take this further?

Several ICO case managers have responded to inquiries about the use of LinkedIn data. They have all stated that LinkedIn, as a public social media platform, is the data controller and therefore has the primary responsibility for ensuring compliance with GDPR. This would include communicating clearly to members how their data will be used as well as being responsible for ensuring data security.

That said, if a LinkedIn member takes data from the platform or shares data with a third party, they then become the data controller and are responsible for complying with any applicable data protection laws.

Individuals join LinkedIn with the expectation other members will communicate and network with each other, so the day to day use of the platform is not necessarily impacted by GDPR.

If you want to continue to use LinkedIn for social selling, it is recommended to focus on expanding your existing network. LinkedIn not only allows you to message your 1st degree connections, as premium subscribers can also contact 2nd and 3rd degree connections.

1. This memorandum is intended as a general overview of the subject and cannot be regarded as legal advice.