1. Is there a GDPR certification?

No, currently there is no GDPR certification issued by the European Commission. Salesforce will be monitoring any certifications that are released after the GDPR becomes effective and will get certified, if it deems them to be appropriate.

---

2. What constitutes personal data?

GDPR aims to protect individual's data that includes a wide range of personal identifiers including name, identification number, location data or online identifiers that reflect changes in technology and the way organisations collect information about people. In other words, all those identifiers that helps to identify an individual are included within the definition of 'personal data' for GDPR.

---

3. Do data processors need 'explicit' or 'unambiguous'

data subject consent – and what is the difference?

Yes. The conditions for consent have been strengthened, as companies are no longer able to utilize long illegible terms and conditions full of legalese. The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. This means that it must be unambiguous. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it. Explicit consent is required only for processing sensitive personal data – in this context, nothing short of "opt-in" will suffice. However, for non-sensitive data, "unambiguous" consent will suffice.

---

4. What is the difference between the "right to restrict processing" and "consent management?

The right to restrict processing refers to the right of Data Subjects to request that a data controller blocks or suppresses the processing of their personal data. Consent Management refers to the ability of organizations to manage individual's consent preferences. In order to process personal data, organizations must have a lawful basis to process the data. Under the GDPR, there are six legal bases which

organizations can rely on to lawfully process personal data. One of these is the consent of the data subject. If an organization is relying on consent, and the individual requests a restriction of processing of their personal data, depending on the circumstance of the request, organizations may also consider updating the individual's consent preferences. This change would include their intent to restrict all processing of their personal data. Organizations should seek legal counsel to understand what legal bases they are relying on to lawfully process personal data and their obligations under the GDPR, in order to design their process.

---

5. Who is a Data Protection Officer (DPO)?

A Data Protection Officer is the professional responsible for the data protection activities and measures inside the company. He/she holds the security leadership role in charge of overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

Our information security manager will be our DPO. If you want more details, you can reach out via email at data-protection-officer@screen-magic.com.

---

6. How should we notify customers of these new rights?

The European Commission has a website with guidance for its citizens on GDPR.

---

7. Is Screen Magic GDPR compliant?

Yes, Screen Magic is GDPR compliant.

---

8. What does GDPR mean for customers?

Screen Magic understands that meeting the GDPR requirements may take a lot of time and effort. As your partner, we want to help you make your process as seamless as possible, so you can focus on running your business. Some of our product enhancements will make it easier for you to:

- Provide access controls
- Encrypt, anonymize, or delete user data
- Perform data audits or assessments using data processing logs

- Create provisions for data subjects’ rights
- Enhance security for user data

---

9. How does GDPR impact Screen Magic and its customers?

The GDPR regulates the “processing” of personal data of any EU resident (who is referred to as a “data subject”). “Processing” includes the collection, storage, transfer, or use, of personal data. This means that any company that processes the personal data of any data subject, regardless of where the company is based, is subject to the rules of the GDPR. Additionally, the GDPR defines personal data very broadly, and includes name, email, demographic information, real-time location, online activity, and health information, to name a few. As the messaging service platform, Screen Magic receives billions of data points from all over the globe, including data points that are or contain personal data from data subjects. This means that both Screen Magic and our customers sending us data will need to comply with the requirements of the GDPR.

---

10. Is Screen Magic

collecting data?

Screen Magic is the “data processor” for its customer’s data. Our customers therefore are the “data controller”. These terms are defined under the GDPR. The data controller collects data from data subjects (i.e., customer) and says how and why personal data is processed. The data processor receives the data from the data controller and acts upon instruction from the data controller.

---

11. What data does Screen Magic process?

While registering for our product/services we request you to provide us with such information like the first name, last name, company business name, address, website address, email address. This is the basic data that we process and store. We also store Billing contact (email address), Billing address, shipping address, Contact number for billing, Point Of Contact for rest of the conversation (Name, email, phone), address of the company as well as any additional address to whom invoice needs to be communicated. We also store SMS data that is SMS content and phone numbers. All information is stored in an encrypted format. Along with the business related data, account related information, such as customer ID, company and fields are also stored. You can find a full description of the data processing practices in our Privacy Policy: https://www.sms-magic.com/privacy-policy/

12. Do I need to sign a Data Processing Agreement/Addendum (DPA)?

Yes. Regardless of being a data controller or a data processor, when you transfer the personal data to us (and you do so using our services) you may need to enter into a Data Processing Agreement (DPA) with us if you are transferring any EU citizens personal data.

---

13. Will Screen Magic sign a Data Processing Agreement ("DPA") with me?

Yes. We understand the GDPR has robust requirements and obligations for both data collectors and data processors and we are committed to helping our customers use Screen Magic in a compliant manner. We have made our DPA available online so that our customers can be confident that their data is processed in a lawful manner.

---

14. How should we notify customer of these new rights?

The European Commission has a website with guidance for its citizens on GDPR.

---

15. Can customer data in Screen Magic be encrypted?

Yes. Screen Magic chose to leverage standard encryption to demonstrate their security measures and to serve as an additional layer of precaution against a data breach.

---

16. What level of access does Screen Magic have within the customers’ Salesforce org?

Screen Magic personnel do not have access to our customers’ Salesforce org. Our customer support agents may need temporary access to a customer’s org for troubleshooting or setting up the SMS-Magic platform. Our support agent will only access a customer’s Salesforce org after receiving explicit consent from the customer via email. Customers are recommended to give limited profile access which is only needed for setup and troubleshooting purposes. The SMS-Magic platform has API

access to our customers’ Salesforce org, which is used programmatically for updating SMS transaction data in the customer’s Salesforce org and retrieving SMS aggregate data for quality checks. This API access is granted using OAuth by a particular user of the customer’s org. The SMS-Magic platform will have the same access level as the OAuth user but the platform only accesses SMS-Magic objects. It’s recommended that customers only grant limited access to SMS-Magic users.

---

17. When you delete a person record (Contact / Lead / Person Accounts) from your database, are all the associated records/objects deleted?

Yes. When a person record is deleted from the Screen Magic database, all the associated records are automatically deleted. However, additional steps may need to be taken in order to delete the personal data from other fields, like calendar events, tasks.

---

18. Is your server/data centre located in EU?

Yes, Screen Magic has a data centre in Europe hosted with Amazon AWS in Dublin, Ireland. If you are an existing EU customer of Screen-Magic, you can place a request to move your data from our US data centre to our Europe data centre.

---

19. What is your data retention/deletion policy?

Screen Magic has defined policy for data retention as well as deletion. Customer data is retained for the period of 6 months after which it is archived.

To delete data, customer has to send a data deletion request to security@screen-magic.com. Once proper authentication of the request is completed, the data will be completely erased from the Screen Magic server.

---

20. How do you manage customer consent for sending

text messages?

For SFDC, we have an opt-out and opt-in mechanism you can use.

If you are using our portal to send SMS, you can use the subscription feature to manage customer consent.

You can get in touch with our customer support team at https://www.sms-magic.com/support/.

---

21. How does Screen Magic handle customer data?

For any data handling related queries, you can reach out via email to data-protection-officer@screen-magic.com

---

23. Can I configure a separate consent for Service and Marketing messages?

a. Yes, you can configure a Separate Consent for Service & Marketing Messages using the Content-Type functionality of Consent Management.

b. Consent Management offers features to map Templates to Consent Types, which enables you to categorize consent based

on different content types.

---

22. Can I message recipients who have opted out from one sender ID through another Sender ID?

a. If you have chosen Sender ID as an attribute while setting up consent management, each consent is mapped to a specific Sender ID. If the ‘Opt-Out’ request is received, it will be for that specific Sender ID. You can still send messages using another Sender ID.

b. If you receive a blanket ‘Opt-Out’, you will not be able to send messages using any Sender ID.

---

24. We get consent through our website. Is it sufficient for sending SMS?

It would be sufficient if you are taking explicit consent to send messages via SMS on the Website.

25. Do I need Double Opt-in for sending messages through a shortcode?

Double opt-in is not mandatory but recommended as a best practice. As far as you are taking initial consent to text & have provision to Opt them Out if they want to, Double Opt in is not needed.

---

26. I’m in the U.S. and messaging recipients here, do I need to care about GDPR?

a. Yes,

b. Setup a flow to cater to both TCPA and GDPR compliances. SMS-Magic offers both and it is easy for us to handle it.

---

27. Does SMS-Magic cover TCPA

and GDPR compliant messaging?

SMS-Magic Provides you Compliance Framework that you configure to be TCPA & GDPR Complaint.

---

28. I want to prevent messages going out to known plaintiffs and DND’s. Do you offer that?

No, At this moment we do not have this feature. You need to have a clean database to avoid sending to DND & Plaintiffs.

---

29. Can I take consent on the phone?

Yes you can take Consent on Phone. TCPA / GDPR & Other Compliance Policies require you to maintain a log of how you have taken the consent. As far as you are storing evidence in the form of call task / recording / MOM of call etc, consent on phone can be taken. It is however recommended that you seek consent using Opt In Text so that you have proper logs in your System in the form of incoming messages or Consent Records.

30. I already have consent for sending messages, how do I migrate those into SMS-Magic?

For Version 1.59 & above, Consents are stored as Salesforce Records (Consent Object). You can mass import consent using Dataloader / Workbench. For Versions before 1.59, Consents are marked as Checkbox on associated object record. For example, Opt In field on Lead Object. You can mass update Opt in / Opt out field to mark consent.

---

31. If I receive an incoming SMS from a recipient, how do I know that the recipient has opted in?

You can find out if the recipients have opted in if they have replied with “subscribe”, “Opt-IN” etc. in your previous messages.

---

32. In what situations do I need Double Opt-In?

We would need double opt-in if the customer has filled in the webform and has given consent for receiving messages. It is recommended that we ask for optin in text as well.

---

33. What if I already have consent and I don’t need the Compliance framework?

It is always customers call for compliance but as the best practice, we recommend to use the Compliance framework.

---

34. Are you HIPPA compliant?

Yes, SMS Magic is a HIPPA compliant.

---

35. How to get started with

GDPR, TCPA, CASL and other compliance and avoid unnecessary fines?

SMS Magic is a HIPPA compliant. We can setup the configurations with respect to either the semder ID or the mobile number wise or with both the configurations in salesforce. You can write down to care@screen-magic.com to know more.