OliveFX GDPR OVERVIEW & Compliance Plan

Delivery time: 25th Sept 2018
Responsible unit: S2T

I. AREAS TO NOTE:

1. *The GDPR is applicable when personal data is processed, by which a natural person can, directly or indirectly, be identified – APPLICABLE to OLiveFX.* ***Triggers****:*

   - Name, address, e-mail, DOB, + IP address/Device ID
   - special categories of personal data: photo, biometric data, health, race, religion, gender. Unless gov issued photo ID document, AVOID collecting special category
   - indirect data collection: facebook, linkedin – social media' data aggregation

2. **Key Concepts**:
   - Data Controller (determines what happens with personal data how it's processed),
   - Processor processes the data on behalf of the controller via
   - inhouse IT department = The Controller and the Processor is the same entity
   - outsourced 3rd party = Processing Agreement must be in place between the processor and the controller, outlining the boundaries of data processing. If the processor is acting beyond the set boundaries – automatically becomes responsible & liable by law – potentially costly option, requiring GDPR certification of the outsourced processor, with additional measures to apply to our systems & controls.
   - Data Subject (Customer from EU or hire/contractor from EU)
3. Requirement to have a Data Processing Officer (DPO), email address and contact channel for complaints or any customer communication with regusts to provide their personal data have to be VISIBLE ON WEBSITE (compliance contact details are still valid as compliance officer could act as the DPO)

4. Data protection by design and by default meaning:
   - It's mandatory when designing a new system, process, service, etc. that processes personal data, to make sure that data protection considerations. Organizations need to be able to prove that they have done so.
   - when the system, process, service, etc. to be designed will include choices for the individual on how much personal data he shares with others, the default setting is the most privacy friendly one, so the one that says to not share any information at all. This data protection by default notion further includes data minimization principles.
   - DPO have to keep the records of all processing activities they perform on behalf of clients. A supervisory authority can go to processors directly with requests and demands.
5. Data Protection Impact Assessments (DPIA):
   - ID high risks to the Privacy rights of individuals when Processing the data;
   - Formulate Mitigation to address those risks (systematic description of processing activity and the necessity and proportionality of the operations) –OliveFX Master MANUAL

The DPIA to be performed PRIOR to collecting & Processing Personal Data

6. Security: Risk Assessed

- to ensure the confidentiality, integrity, availability and resilience of processing systems and services
- NEW: Pseudonymized & anonymized data – assumed not to be Personal Data, however, it is under GDPR, unless the anonymized data is "irreversibly" encrypted (very hard to prove): after data is encrypted, the key must be discarded, and all data that can be redirected to a particular person has disappeared.

7. Cloud service providers, "over the top services" (WhatsApp, Skype etc), phone call, paper letters, voice messages, i-messaging & webmail services – all fall under GDPR. The cloud service provider cannot do anything with your data, unless you instruct them to do so and the data remain within your controllership. Have precise retention period stipulated. Back ups.
8. Metadata is included in GDPR (location data, time and duration of conversation giving insight in private life)
9. Cookies: Cookies may be used when
   (1) this is necessary for transferring the data,
   (2) or if it is required to provide the requested services,
   (3) when it is necessary for measuring web statistics (first party cookies), or
   (4) when consent was given by the data subject.

For the obtained consent (clear, explicit and non-binding) - strict requirements apply. Clear possibility to opt out must be given to investors. For tracking cookies consent is required prior to the placement of these third party cookies

10. Personal Data breach mgt: must define the breach(s) & time period to report. Multi country cloud strategy.
    Notification: ": in case (preventive) security measures are breached and personal data is unlawfully processed, the controller must report such a breach to the supervisory authority within 72 hours, and possibly to affected data subjects as well. This is the case unless you can establish that the breach has caused no actual risks for the data subjects or other individuals. – reporting after the breach mgt actions taken within (prevent, detect & respond) in all cases in accordance to designed Security Response Plans, stipulating roles and responsibilities, process description, checklists etc.
11. Clear policies, guidelines and work instructions related to data protection should be developed and a privacy specialist should be available to assist in applying these requirements.
12. Data Controllership/Ownership must be spelled out in the contract with customers, i.e. we must confirm that, according to the host-countries' laws, the company retains ownership of the transferred data.
13. IT Security and privacy: measures or certifications the provider has in place. Cloud providers can demonstrate compliance with security and Privacy by Design in several ways:
    - With the results of a performed DPIA;
    - By being ISO 27001 certified (information security management system);
    - By being ISO 27018 certified (code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors).
14. Create a central register for the records: excel spreadsheets (?) or any other centralized tools to provide a full overview of the processing activities that take place within the organization. Tech measures to incl:
    - access and authorization rights (not everyone should be authorized to change or alter information).

II. ACTIONS / SAFEGUARDS:

1. Publish full Contact Information
   - Compliance@olivefx.com, CS@olivefx.com, info@olivefx.com
   - Physical address, Phone numbers, Chats etc

2. Trading & Office Hours conditions

3. Disclaimers:

3.1 "This website is owned and operated by xxxxxxxxxx. Registered office, Company no xxxxxxxx AFSL No xxxxxxxxx. Xxxxxxxxxxx(OliveFX) is a trading name of xxxxxxxxx (OFM) wo is authorized and regulated by Australian Securities and Investments Commission (ASIC) in Australia. The information and content provided on the website (the Information") you are going to access, has been compiled and presented in accordance with Australian laws and regulations and applicable and legitimate basis for cross-border data security and protection laws.
The Information is not intended for distribution to, or use by, any person or entity in any jurisdiction or country where such distribution or use may be contrary to any of the laws or regulations of that jurisdiction. The products and services described herein may not be available in all countries and jurisdictions. Those who access this site do so on their own initiative, and are therefore responsible for compliance with applicable local laws and regulations. The release does not constitute any invitation or recruitment of business.
xxxxxxxxxx does not offer its services to residents of certain jurisdictions such as
Afghanistan, Belgium, Central African Republic, Democratic Republic Congo, Eritrea, Iran, Iraq, Israel, Libya, North Korea, Somalia, South Sudan, Syria, USA, and Yemen[1]

3.2 Data Protection Rights: Links to Legal Page to include (ANNEX 1):

1) "What Type of Personal Data We Collect and How We Collect It?"
2) "How We Use Your Personal Information?"
3) "Disclosure of Personal Information"
4) "Security of Personal Information"
5) "Retention period or criteria used to determine the retention period"
6) "Data Subject Rights"
7) "The Rights to Lodge a Complaint"

4. Push notifications:

4.1 "Stay Current": "*We would like to show you notifications for the latest news and updates*":
   - "**No thanks**"
   - "**Allow**": action

---

[1]Prohibited regions (TBC) – regulatory reasons; Sanctioned (by OFAC and/or HM Treasury & Other Prohibited Countries, https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx

Action pop up window template:

"Sign up to receive xxxxxxxxxx (latest news and trends) from XXXXXXXX directly to your inbox for 30 days:

First name: [redacted]

Last name:
*Email address: (**Privacy Notice**)*
Confirm Email address:
Phone number:

"I would lie to receive xxxxxxxxxx, company news and information about OliveFX' products and promotions via email, customer portal and/or phone

Tick boxes for explicit consent:

Yes ☐ No ☐

SUBSCRIBE

Your Data is Safe with us. Please refer to our *(**Privacy Notice*** link (**ANNEX 2, para 1**)

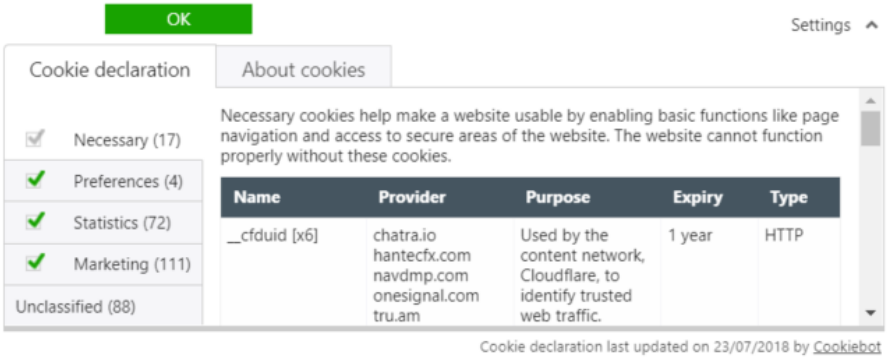
4.2. Have "**Unsubscribe**" link on communication channel (incl on every outgoing MKT based email)

4.3. Cookies

- disclose a tracking technology company if any (for ex, Cookiebot, updates cookie declarations automatically)
- **Mandatory Cookies Disclaimer,** as per template:

"*We use cookies to personalize and optimise content to improve our services, to provide social media features and to analyse our traffic. We process this information about use of our site with our analytics partners who may combine it with other information that you've provided to better our services. You consent to our cookies if you continue to use our website. For more information visit **Cookie page*** (**ANNEX 2, para 2**) *and read our updated **Privacy Notice**."*

- OK
- **Settings:** link to a pop up informative window ex,



5. Risk Disclosures (ANNEX 3)

6. **Terms & Conditions** to cater for provisions as per **ANNEX 4 (TBC)**

7. **Key Information Documents** (TBC)

8. Publish:
    - Execution policy
    - Conflicts Policy
    - Complaints Procedure
    - Treating Customers Fairly