SUBJECT ACCESS REQUEST (SAR) MANAGEMENT

Best Practices Checklist

Whether you're reacting to a flood of subject access requests or want to develop competitive advantage by giving your customers easy access to all their data, SARs will be a fact of life. There is really no way to predict the number of access requests that any particular company will receive, but all indications point to one common answer: many more than you've ever had to deal with before.

It's one thing to plan for the GDPR or CCPA and other privacy regulations. It's another thing to actually live it. What does it actually feel like day to day? What do you actually have to do to operationally support the GDPR, the CCPA, or other regulations still to come?

This checklist is designed to help you comply with today's regulations, anticipate and react to regulations on the horizon, reduce confusion and noise created by data subjects' requests for information, and stay flexible enough to react efficiently to the inevitable changes to come.

The Plays referenced here are part of the SAR Management Best Practices Playbook.

PLAY 1

Comply from the point of collection

- □ Before you collect any personal data, explain why you're collecting it and what you will do with it
- □ Obtain explicit and informed consent from data subjects
- □ Explain your general disclosure policies
- □ Articulate the rights of your data subjects on what data you collect and how you use it
- □ Explain processes available for subjects to exercise those rights
- □ Articulate cookies and opt-out procedures
- □ Explain your relationships with sub-processors, affiliates, and others with whom you share subjects' data
- □ Create a centralized place where consent and disclosures (including versions) are tracked

PLAY 2

Maintain process/technology flexibility

- □ Whatever solution you implement, ensure it is flexible to adapt as existing regulations are modified and new ones are enacted
- □ Be prepared for new interpretations of reporting requirements
- □ Stay tuned for specifics on data portability
- □ If you build your own solution, budget extra IT hours

PLAY 3

Eliminate unstructured requests

- □ Eliminate unstructured requests by directing subjects to a web form or privacy portal rather than taking requests by email (this can cut your overhead by 10-20%)
- □ Set up CAPTCHA to help eliminate robots and limit spam
- □ Leverage a portal strategy to give your team – and your data subjects – more control
- □ Consider the portal to also communicate disclosures, past consent, and other information data subjects may expect in one place
- □ Spend time to delight your users with a good experience; perceived transparency helps generate brand trust

truyo™

Privacy Rights. Automated.

PLAY
4

Validate user identity

- □ Automate where possible, and wherever you can justify it, to manage high volumes of requests; at the very least, implement CAPTCHA to filter out the robots
- □ Send confirmation links to email addresses and/or mobile numbers *before* you show data linked to those assets
- □ Consider incorporating 3rd party validation services
- □ Consider authenticating current customers and employees with your LDAP, OAuth, or SAML authentication systems (but don't forgot non-customers have rights, too)
- □ Think carefully about requiring the user to upload a photo ID – you're then responsible for that data, and it introduces a potentially manual step to your SAR operation

PLAY
5

Simplify consent management

- □ Be specific without being overwhelming
- □ Consider a matrix of consent to manage the complexity of multiple agreements
- □ Manage consent documents in different versions and languages
- □ Create a simple ledger to record when consent is granted

PLAY
6

Control requests to be forgotten

- □ Support deletion of specific data elements or groupings as the primary action
- □ "Delete all data" should always be a secondary action
- □ Remind users of the services and/or value (e.g., loyalty points) they will lose if they delete their data
- □ Anonymize or pseudo-anonymize rather than delete (regulations allow you to retain a minimum set of data in order to maintain compliance with requests to be forgotten)
- □ Consider creating an API and/or automated routine to help catch "forgotten" data elements before you accidentally use them again; the API/routine should tie back to your privacy tasks to auto-alert data source owners to delete records

PLAY
7

Demonstrate compliance

- □ Anticipate audits of your processes *and* your performance
- □ Develop a system to report on request types, results, and response timeframes
- □ Prepare for exporting and summarizing your processes and workflows
- □ Reporting requirements are still a regulatory gray area – so don't over-engineer your response
- □ Budget IT hours to scope and maintain adherence
- □ Consider blockchain which allows you to create an immutable ledger
- □ Be able to respond to a regulator's inquiry within 48 hours

PLAY
8

Automate

- □ Eliminate human effort (and errors) where possible; at the very least, automate validation and workflow management
- □ Automate data searching/identification, collection/extraction, packaging/presentation, and reject requests by centralizing or indexing all of your data
- □ Consider a data lake strategy as an easier way to centralize your data without taxing your IT team
- □ Automate changes to original data sources (that can eliminate the remaining 50-95% of your overhead)
- □ Remember that implementing a portal alone, while a good first step, is not automation

Download the SAR Management Playbook to learn more about these best practices

Truyo is a collaboration between Intel® and IntraEdge to bring scalable privacy rights and SAR automation to the enterprise. Truyo is an Intel® Market Ready Solution. To learn more, visit truyo.com