G D P R

A USER'S BILL OF RIGHTS FOR A DATA-DRIVEN ERA

The GDPR protects individuals' data rights within the EU. Every business with a website or digital advertising campaign has obligations. For brands and advertisers it can be confusing. The Media Trust knows what you need to do.

BRAND ADVERTISER RESPONSIBILITIES

GET DATA SMART

Be prepared to identify and document all data elements — collected, used, stored, shared. Brands should pay particular attention to third-party agencies, technologies, and processes including CRM, direct marketing and website operations.

EVALUATE PRIVACY RISKS

Brand advertisers should conduct Data Privacy Impact Assessments (DPIAs) to evaluate privacy risks. It's also good practice to implement 'Privacy by Design' approaches to everyday site operations, such as minimizing & pseudonymising data.

HAVE A LAWFUL BASIS

Heads up: brand advertisers will need a legal basis to process personal data, especially data collected via brand sites and campaign landing pages. Legal basis depends on the type and nature of the data processing, e.g., data collection v. data analysis. 'Consent' and 'Legitimate Interests' are the key legal bases for digital marketing.

KEEP AN APPROVED PARTNER LIST

You're only as trustworthy as the company you keep. Brands are ultimately responsible for the actions of their downstream digital business partners when it comes to proper data treatment--from ad campaign targeting to landing pages. But note: the GDPR establishes joint liability for all companies in the supply chain, with or without a data privacy agreement.

BE ON TOP OF DATA BREACHES

If brands don't already have one, they must design and test a process to identify and report a data breach. If and when a breach occurs, the relevant regulator must be notified within 72 hours and, in some circumstances, the user, depending on the nature of the breach.

MAINTAIN TRANSPARENCY

GDPR is all about clarity. Users must be clearly informed about personal data collection activities including the specific data elements, what entities have access to it, and how that data will be used. This must occur at the point of data collection and be spelled out in the website's Privacy Notice.

ABOVE ALL ELSE

The user's individual rights must be respected and prioritized. Brands must put in place processes and procedures to give users greater control over their personal data, such as giving them to right to 'port' their personal data.

ALL USERS HAVE THE RIGHT:

1. **TO BE INFORMED**
   Gives the user greater transparency over how personal data is used
2. **TO RESTRICT DATA PROCESSING**
   Allows the user to block or suppress personal data processing in certain circumstances (e.g., when the user contests the accuracy or lawfulness of the personal data)
3. **TO NOT BE SUBJECT TO AUTOMATED DECISION-MAKING**
   Provides protection to users if automated decision-making, including online profiling, has a legal or similarly significant effect on them
4. **TO DATA PORTABILITY**
   Enables users to obtain and reuse their personal data for their own purposes across different services
5. **TO OBJECT TO DATA PROCESSING**
   Allows users to stop the processing of their personal data at any time
6. **TO ERASE THEIR PERSONAL DATA**
   Respects a user's request to delete or remove their personal data being processed
7. **TO ACCESS THEIR PERSONAL DATA**
   Provides a user with access to their personal data
8. **TO RECTIFICATION**
   Allows a user to correct inaccurate or incomplete personal data

PUBLISHER RESPONSIBILITIES

GET DATA SMART

Be prepared to identify and document all data elements — collected, used, stored, shared. Publishers should keep a critical eye on upstream ad/martech partners.

EVALUATE PRIVACY RISKS

Publishers should conduct Data Privacy Impact Assessments (DPIAs) to evaluate their privacy risks. It's also good practice to implement 'Privacy by Design' approaches to everyday site operations, such as minimizing & pseudonymising data.

HAVE A LAWFUL BASIS

Publishers will need a legal basis to process personal data. Legal basis depends on the type and nature of the data processing. 'Consent' and 'Legitimate Interest' are the key legal bases for digital marketing.

KEEP AN APPROVED PARTNER LIST

You're only as trustworthy as the company you keep. Publishers are ultimately responsible for the actions of their upstream digital business partners when it comes to proper data treatment. But note: the GDPR establishes joint liability for all companies in the supply chain.

BE ON TOP OF DATA BREACHES

If they don't have one already, publishers—as well as their partners/advertiser clients—must design and test a process to identify and report identify and report unauthorized collection of consumer data via your media property. If and when a breach occurs, the relevant regulator must be notified within 72 hours and, in some circumstances, the user, depending on the nature of the breach.

MAINTAIN TRANSPARENCY

GDPR is all about clarity. Users must be clearly informed about personal data collection activities including the specific data elements, what entities have access to it, and how that data will be used. This must occur at the point of data collection and be spelled out in the website's Privacy Notice and cookie disclosure.

ABOVE ALL ELSE

The user's individual rights must be respected and prioritized. Publishers must put in place processes and procedures to give users greater control over their personal data, such as giving them to right to 'port' their personal data.

THE MEDIA TRUST

The first step to satisfying your GDPR obligations is knowing your digital ecosystem—identify, analyze, communicate and enforce. Ask The Media Trust how you can operationalize compliance for your digital properties.