MDDM
Data Protection

WEBSITE OR DEVICE COOKIE CHECKLIST

Cookies & tracking technology on any device that connects to the internet eg website, phone, laptop or IoT

COOKIE POP-UP OR BANNER STATEMENT

As the user lands on your site	Ensure a Cookie Permission statement is clearly visible, such as a pop-up or a permission banner (using your preferred design & wording format)
Consent or Reject	Using plain language, briefly explain that the device uses cookies with the option to 'Accept All' or provide "More Information'
Equal Importance	'More Information' button must have equal visibility to the user as "Accept'
Privacy & Cookie Policy	Ensure the banner does not obscure the access to your Privacy or Cookie buttons
Access to Cookie Policy	If you choose to insert the Cookie Policy link within the Banner statement, ensure it is still available to view when the banner disappears
Accept or Reject	Suggest you do not offer 'Accept' or 'Reject' only. As Reject must reject ALL cookies that are not 'Strictly Necessary', which may reduce 'user experience' unnecessarily (user may be happy with YouTube plug-in but not Google Analytics)
'X' or Ignore	X out, no action or pop-up simply disappears cannot be taken as consent. Cookies cannot be activated until user has actively consented to the use
Consent by Implication	It is not permissible to assume consent eg "By continuing to use this website, cookies will be activated'
User-friendly Consent	The user must be able to withdraw consent as easily as they gave it

ALL ORGANISATIONS BASED IN IRELAND HAVE BEEN GIVEN UNTIL 6TH OCTOBER 2020 TO BRING THEIR TECHNICAL DEVICES SUCH AS WEBSITES, MOBILE APPS AND IOT INTO COMPLIANCE WITH E-PRIVACY REGULATION & GDPR BEFORE ENFORCEMENT & FINES COMMENCE.

Prepared by maeve@mddm.ie Data Protection Officer.
Revised e-Privacy Regulation from the Irish Data Protection Commission (April 2020)

Define your Cookies – Functional

Strictly Necessary	Strictly necessary cookies enable core functionality, such as security, network management and accessibility.
Explicitly Requested	Necessary cookies also cover explicitly requested functions eg shopping basket tracking
No Consent Required	These are the only cookie functions that do not require consent eg they can have a pre-ticked box or slider set to ON
Turn off at Browser	Offer the user the ability to disable at browser settings, warning this will affect the website function
Indefinite Expiry Date	Check 'expiry' date such as session cookies. They should not have an indefinite expiry date and should be set to expire when or shortly after it has served its function eg ticket purchase
Defining Necessary	The definition of necessary is tight and does not simply apply to improved user experience. Document your definition & decision, ideally in your Cookie Policy
Bundle Consent	You can 'bundle' all necessary cookies although they may have different functions

E-Privacy Regulation applies to the use of all Cookies that store or track any information both identifiable (personal data) or anonymised/aggregated data.

Define your Cookies – Non-Functional

Not strictly necessary	Although they may enrich the user experience and may appear as basic functions, all other Cookies are non-functional and all need consent
Active Consent	The user must actively opt-in. No "pre-ticked' boxes or sliders set to ON
Activation upon Consent	All non-functional cookies must remain OFF until consent has been received eg a 'chat box' cannot be deployed until consent is received
Bundle Consent	You cannot 'bundle' consent for multiple functions. Consent is not required for every Cookie but for every purpose.

Turn off at Browser	The option to disable non-necessary cookies at the user's own browser cannot be the only option given to the user
Expiry Date	Ensure all non-functional cookies have a clear expiry date and the lifespan should be outlined in the Cookie Policy for transparency
Analytics	All analytics require consent either internal tracking or third-party tracking eg Google analytics. This includes the use of personal or annonoymised data
Customer Journey	A suggested option would be to introduce pop-up consent during the customer journey and before they access a specific function eg BrowseAloud for text-to-speech functionality or YouTube before you demonstrate a product.
Privacy-enhanced	A suggestion, if you embed videos from channels such as YouTube, you may wish to limit activity to your own official channel where you can control settings. Consider using privacy-enhanced mode, where possible.
Re-confirm Consent	Ensure appropriate controls are in place to track and update consent and preference changes. Re-confirm consent after a set period of time - suggested time-frame 6 months

EXAMPLES OF COOKIES THAT REQUIRE CONSENT

Mailchimp	Any campaign management tool that tracks email campaigns, such as open rates, bounces
IP Address	IP tracers to identify and track IP addresses are tracking personal data and these cookies are covered under both GDPR & e-Privacy regulation
Location ON	Location tracking or 'local' store location. Asking the user to switch Location ON
Facebook	Links to your organization's official social media channels or social activity such as 'like' or 'Share'

Action Steps

Cookie Audit	Ask IT or MDdm to carry out a Cookie Audit. You may well be surprised what you locate 'under the bonnet'
Define Cookie Type	Define & document strictly necessary & non-necessary cookies. Outline, in summary, in your Cookie Policy
Expiry Dates	Check your cookie expiry dates and ensure non-functional or session cookies have an appropriate date stamp. Display this in your Cookie Policy
Consent	Review your consent statement and update or implement a 2nd step Cookie Review & Consent
Cookie Policy	Review & update your Cookie Policy / Statement to ensure it meets new regulation guidelines
Record of Processing	Under GDPR, carry out a yearly Data Audit (ROP) of your website that sits alongside your Cookie Audit to track the process of data in and out of the website
DPIA	Review the need to carry out a Data Protection Impact Assessment (DPIA) for the use of Cookies and processing of personal data
Privacy Setting	Check privacy settings & privacy policies from third-party plug-ins
Responsibility & Liability	Check your contracts with all third-party plug-ins. Do you remain the Controller (responsible) or are you joint-Controller (shared responsibilities)? Do you have appropriate Data Processing Agreements (DPA's) in place?

As your Data Protection Officer or Data Privacy Consultant, we are here to answer any questions you may have or any concerns in relation to changes in regulation. We are happy to work with you to implement privacy-friendly changes to your communication strategy.