NuSpark Media Group

GDPR CHECKLIST

INITIAL EMAIL

Checklist	Rationale	How
- Obtain explicit consent before sending emails.	GDPR requires clear and unambiguous consent for all direct marketing communications.	Use an opt-in form with a clear consent checkbox that is not pre-checked, and store consent records securely.
- Avoid using pre-checked consent boxes.	Pre-checked boxes do not meet GDPR's standard of explicit consent.	Configure form settings to ensure checkboxes are unchecked by default.
- Clearly state the purpose of the email (e.g., promotional, informational).	Transparency ensures users understand the intent of your communication, aligning with GDPR requirements.	Include a short explanation at the sign-up stage and reiterate the email's purpose in the email body (e.g., "You subscribed for updates about...").
- Include the sender's identity and contact information in the email footer.	GDPR mandates that recipients must be able to identify and contact the sender easily.	Add your company name, address, and support contact details (e.g., email, phone) in the footer of every email.
- Provide a visible and simple way to unsubscribe.	GDPR gives individuals the right to withdraw consent at any time, making an unsubscribe option mandatory.	Include an unsubscribe link in the email footer that redirects users to confirm their opt-out.
- Keep a record of when and how consent was obtained for each recipient.	Demonstrates accountability and compliance with GDPR if audited.	Use a CRM or consent management system to log timestamps, IP addresses, and consent language.
- Avoid sending emails to individuals who have opted out.	Respecting user preferences aligns with GDPR and prevents potential complaints or legal action.	Regularly update your email list to remove opted-out recipients and use suppression lists to avoid accidental re-sends.
- Verify that your email platform is GDPR-compliant and secure.	Ensures that personal data used for emails is processed securely and lawfully.	Use a reputable email service provider (e.g., Mailchimp, HubSpot) that complies with GDPR and provides encryption for stored data.

NuSpark Media Group

GDPR CHECKLIST
CONSENT LANDING PAGE

Checklist	Rationale	How
- Clearly state the purpose of data collection and its intended use.	Transparency ensures users understand why their data is being collected and how it will be used, meeting GDPR requirements.	Add a clear, concise statement above the consent form or checkbox, such as "We collect your data to provide tailored offers and updates."
- Avoid bundling consent with terms and conditions.	GDPR requires that consent is freely given and not tied to other services or agreements.	Separate consent requests from terms acceptance by using independent checkboxes. Ensure each checkbox has specific and distinct wording.
- Use clear and straightforward language, avoiding legal jargon.	Ensures users can easily comprehend the information, supporting informed decision-making.	Write consent-related text at a reading level suitable for a general audience. For example, avoid phrases like "data processing activities" and instead use "how we use your data."
- Include separate checkboxes for different consent types (e.g., marketing, analytics).	Enables users to provide specific consent for different data processing activities.	Add individual checkboxes for purposes like marketing emails and analytics tracking, each with its own description, e.g., "I agree to receive marketing updates."
- Avoid pre-checked boxes for consent options.	Pre-checked boxes do not comply with GDPR's standard of explicit consent.	Ensure all checkboxes are unchecked by default when the page loads. This can be managed via HTML form settings (<input type="checkbox" />).
- Provide a link to the full privacy policy for more details.	Allows users to access comprehensive information about how their data will be handled.	Include a hyperlinked statement like "Learn more about our data use in our Privacy Policy" near the checkboxes or consent forms.
- Include a mechanism for users to withdraw or modify their consent at any time.	Ensures compliance with GDPR's requirement for easily revocable consent.	Offer an account dashboard or email link where users can update or revoke consent. Clearly communicate this option on your website and in emails.
- Keep records of user consent, including timestamp, purpose, and method.	Demonstrates accountability and compliance, which is critical in case of audits or complaints.	Store consent data in a secure database, including the timestamp, IP address, and details of what was agreed to. Use a CRM or consent management platform for tracking.
- Ensure the landing page is accessible across devices and meets usability standards.	Guarantees that all users, regardless of device or ability, can provide informed consent, aligning with GDPR's fairness principle.	Test the page on multiple devices (mobile, tablet, desktop) and use accessibility tools to ensure compliance with WCAG 2.1 guidelines.

NuSpark Media Group

GDPR CHECKLIST

PRIVACY POLICY ADDENDUM

Checklist	Rationale	How
- Clearly specify that the addendum addresses GDPR compliance.	Transparency ensures users understand the purpose of the addendum and its relation to GDPR.	Add an opening statement such as, "This addendum supplements our Privacy Policy and outlines how we comply with GDPR."
- Define how personal data is collected, stored, and processed.	Users must understand how their data is handled to align with GDPR's transparency requirements.	Include sections on the types of data collected, the purposes for collection, and storage methods, using simple language.
- Specify the lawful basis for data processing (e.g., consent, contract, legitimate interest).	GDPR requires businesses to disclose the legal grounds for processing personal data.	Create a section listing lawful bases for each type of processing (e.g., "We process email addresses for marketing based on your explicit consent").
- Explain data subjects' rights (access, rectification, erasure, restriction, portability, objection).	Individuals must know their rights under GDPR and how to exercise them.	Include a user-friendly explanation of each right, along with clear instructions on how to make a request (e.g., via email or a web form).
- Identify third-party vendors or processors involved in data handling.	Users need to know who else may access their data and what safeguards are in place.	List key third-party processors (e.g., payment processors, cloud providers) and link to their privacy policies where applicable.
- Provide details about data retention policies.	Users should know how long their data will be stored and why, ensuring compliance with GDPR's data minimization principle.	Specify retention periods for each type of data (e.g., "We retain transactional data for 7 years to comply with legal obligations").
- Address international data transfers and safeguards.	GDPR mandates protections for transferring personal data outside the EU.	Mention mechanisms like Standard Contractual Clauses (SCCs) or adequacy decisions and specify any countries where data is processed.
- Include an effective date and process for notifying users of changes.	Keeps users informed of updates to privacy practices, fostering trust and compliance.	Add a statement such as, "This addendum is effective as of [date]. Any updates will be posted on our website and communicated where appropriate."
- Provide contact information for data inquiries.	GDPR requires businesses to offer a way for users to reach out regarding data processing or to exercise their rights.	Add a dedicated contact email (e.g., privacy@[yourcompany].com) and/or mailing address in a clearly visible section of the addendum.

NuSpark Media Group

GDPR CHECKLIST

PRIVACY POLICY TEMPLATE

Privacy Policy Addendum for GDPR Compliance
Effective Date: [Insert Date]
At COMPANYX, we are committed to protecting your personal data and ensuring transparency about how we handle your information. This addendum supplements our existing Privacy Policy and specifically addresses our compliance with the General Data Protection Regulation (GDPR).

1. Data Collection and Usage
We collect and process personal data for the following purposes:
To provide and improve our products and services.
To send promotional communications (with your consent).
To comply with legal obligations.
The types of data collected include:
Name, email address, phone number, and payment information.
Usage data, such as IP addresses and browser types (via cookies).

2. Lawful Basis for Processing
We process your data under these lawful bases:
Consent: For marketing emails and optional data collection.
Contractual Necessity: To fulfill agreements, such as order processing.
Legitimate Interests: For fraud prevention and business analytics.

3. Your Rights as a Data Subject
As an individual under GDPR, you have the following rights:
Access: Request a copy of the data we hold about you.
Rectification: Request corrections to inaccurate or incomplete data.
Erasure: Request deletion of your personal data, subject to legal exceptions.
Restriction: Request limitations on how your data is processed.
Portability: Request a copy of your data in a machine-readable format.
Objection: Object to processing based on legitimate interests or direct marketing.
To exercise your rights, contact us at privacy@companyx.com.

4. Third-Party Data Sharing
We may share your data with trusted partners, such as:
Payment processors to complete transactions.
Marketing platforms to send promotional messages (with your consent).
Service providers ensuring secure storage and hosting.
All third parties adhere to GDPR standards.

5. Data Transfers Outside the EU
When transferring data outside the European Economic Area (EEA), we ensure safeguards are in place, such as Standard Contractual Clauses or adequacy decisions.

6. Data Retention
We retain personal data only as long as necessary to fulfill the purposes outlined above or as required by law. For example:
Transactional records: 7 years (legal requirement).
Marketing data: Retained until consent is withdrawn.

7. How to Contact Us
If you have any questions or concerns about this policy or wish to exercise your GDPR rights, please contact us:
Email: privacy@companyx.com
Address: [Insert Address of COMPANYX]
Phone: [Insert Contact Number]

8. Updates to This Addendum
This addendum was last updated on [Insert Date]. Any updates will be posted on our website and communicated where applicable.

NuSpark Media Group

GDPR CHECKLIST

DOUBLE OPT-IN EMAIL

Checklist	Rationale	How
- Send a confirmation email immediately after the user signs up.	Ensures the email address provided is valid and belongs to the user, preventing unauthorized sign-ups.	Use your email service provider (e.g., Mailchimp, HubSpot) to automate the sending of a confirmation email immediately after form submission.
- Clearly state the purpose of the confirmation email.	Transparency helps users understand why they are receiving the email, meeting GDPR's requirement for informed consent.	Include a statement such as, "We need to confirm your subscription to ensure we have your permission to send emails."
- Include a clear call-to-action (CTA) to confirm subscription.	Simplifies the process for users to complete their subscription, reducing friction and aligning with GDPR's standard for explicit consent.	Add a prominent button or link, e.g., "Click here to confirm your subscription," that redirects to a confirmation page.
- Provide a brief summary of what the user is signing up for.	Reinforces informed consent by reminding users of the benefits or content they will receive.	Add a short message like, "By confirming, you'll start receiving our monthly updates, exclusive offers, and CRM tips."
- Use a secure, unique confirmation link that expires after a set period.	Protects against unauthorized access and ensures timely responses from users, enhancing data security.	Generate a token-based link with an expiration period (e.g., 48 hours) and validate it server-side upon user click.
- Store proof of double opt-in, including timestamps and IP addresses of sign-up and confirmation.	Demonstrates accountability and compliance with GDPR if audited.	Use a CRM or database to log the user's sign-up details, including their IP address, timestamps, and actions taken (e.g., clicking the confirmation link).
- Ensure the confirmation email includes the sender's identity and contact information.	Helps users recognize the source of the email and builds trust by meeting GDPR's transparency requirements.	Include your company name, physical address, and support contact (email or phone) in the email footer.
- Provide a link to the privacy policy.	Allows users to understand how their data will be used, fostering transparency and compliance with GDPR.	Add a hyperlink to your privacy policy with text like, "Learn more about how we handle your data in our Privacy Policy."
- Do not add users to the mailing list until they click the confirmation link.	GDPR requires explicit consent to be confirmed before processing personal data for marketing purposes.	Configure your email service provider to only move users to the active subscriber list after the confirmation link has been clicked.

NuSpark Media Group

GDPR CHECKLIST
LEAD MAGNET EMAIL

Checklist	Rationale	How/Example
- Use a truthful, non-misleading subject line that reflects the email content.	GDPR prohibits deceptive practices; recipients must clearly understand the purpose of the email.	Subject line example: "Your Free CRM eBook: Actionable Tips to Streamline Your Workflow."
- Address the recipient by name, if available.	Personalization builds trust and helps ensure the email is perceived as relevant and expected.	Use merge tags in your email platform (e.g., "Hi [First Name], here's your guide.")
- Begin the email by reminding the recipient of their consent and how they signed up.	Reinforces compliance and builds trust by showing that the email aligns with their preferences.	Example: "You're receiving this email because you subscribed to our newsletter and requested our CRM eBook."
- Clearly describe the value of the eBook or offer.	Transparency ensures recipients understand the purpose of the email and encourages engagement.	Example: "Our free eBook will help you implement strategies to improve customer retention and automate workflows."
- Include a visible and clear call-to-action (CTA) to download the eBook.	A straightforward CTA improves user experience and ensures recipients can easily access the promised content.	Example: "Click here to download your eBook" with a prominent button or hyperlink.
- Provide a link to your privacy policy in the email footer.	GDPR requires transparency about data use and ensures recipients can access detailed information about their rights.	Add a footer statement: "Learn more about how we use your data in our Privacy Policy" with a hyperlink.
- Include a clear and functional unsubscribe link.	GDPR mandates an easy way for recipients to withdraw consent at any time.	Add a visible footer link, e.g., "Click here to unsubscribe from these emails."
- Ensure the sender's name and contact information are visible in the email.	GDPR requires transparency about who is sending the email and provides recipients with an easy way to contact you.	Include your company name, address, and a support email or phone number in the email footer.
- Use a GDPR-compliant email service provider.	Ensures the security of personal data and compliance with GDPR requirements.	Use platforms like Mailchimp, HubSpot, or ActiveCampaign, which support GDPR compliance features like consent tracking and data encryption.
- Store records of consent, including the date and method of opt-in.	Demonstrates compliance and provides proof in case of audits or disputes.	Use your CRM or email platform to store consent details, including timestamps, IP addresses, and the specific content of the consent form.

NuSpark Media Group

GDPR CHECKLIST
ADS AND EBLASTS

Checklist	Rationale	How/Example
- Ensure recipients of eBlasts have opted in to receive marketing communications.	GDPR requires explicit consent for sending marketing communications to individuals.	Collect consent via subscription forms with an unchecked opt-in box, clearly stating what the user is agreeing to receive.
- Avoid using purchased lists unless proof of explicit consent for your specific campaign is available.	Purchased lists often lack GDPR-compliant consent, risking non-compliance.	Use consent verification tools to ensure lists meet GDPR requirements, or avoid using purchased lists altogether.
- Clearly identify your company and the purpose of the ad or communication.	Transparency helps recipients understand who is contacting them and why, ensuring compliance with GDPR principles.	Include a visible "Sponsored by [Company Name]" label in the journal ad or at the top of the eBlast email.
- Include a visible and functional unsubscribe link in eBlasts.	GDPR mandates an easy mechanism for recipients to withdraw consent at any time.	Add an "Unsubscribe" link at the bottom of every eBlast email that leads to a confirmation page or email preference center.
- Use GDPR-compliant targeting methods for journal ads (e.g., anonymized or aggregated data).	Protects individuals' personal data and aligns with GDPR requirements for lawful processing.	Configure ad platforms to use aggregated audience insights instead of personally identifiable information (PII).
- Provide a link to your privacy policy in the ad or eBlast.	Ensures transparency about how user data is handled and their rights under GDPR.	Include a line such as "Learn more about how we handle your data in our Privacy Policy" with a clickable link.
- Verify that third-party platforms or partners involved in ad delivery comply with GDPR.	GDPR requires accountability for any third parties processing personal data on your behalf.	Use Data Processing Agreements (DPAs) with ad platforms or media partners, ensuring they meet GDPR requirements.

NuSpark Media Group

GDPR CHECKLIST RETARGETING

Checklist	Rationale	How/Example
- Obtain consent for cookies or similar tracking technologies before enabling retargeting.	GDPR requires explicit consent for using cookies to track behavior for targeted advertising.	Display a cookie consent banner that allows users to accept, reject, or customize their preferences for tracking.
- Clearly explain how retargeting works in your privacy policy.	Transparency about data use builds trust and aligns with GDPR's principles.	Include a section in the privacy policy titled "How We Use Cookies and Retargeting" with examples of what data is collected and how it is used.
- Allow users to opt out of tracking or retargeting.	GDPR gives individuals the right to control how their data is used.	Provide a cookie settings page or link to opt-out tools like YourAdChoices or the Network Advertising Initiative.
- Use anonymized or pseudonymized data for retargeting campaigns.	Reduces privacy risks by ensuring personal data is not directly exposed or used for targeting.	Configure ad platforms to only use non-identifiable audience segments for retargeting campaigns.
- Verify that third-party platforms (e.g., Google Ads, Meta) comply with GDPR.	GDPR requires that all data processors used in retargeting meet compliance standards.	Work with GDPR-compliant platforms that provide features like consent mode (e.g., Google Consent Mode) and ensure DPAs are in place.
- Provide users with information about how their data is used for retargeting.	Transparency helps individuals understand and control how their data is being processed.	Add text to the cookie consent banner and privacy policy, e.g., "We use cookies to show you personalized ads based on your browsing activity."
- Store data only for as long as necessary for the retargeting campaign.	GDPR requires data minimization, meaning data should only be retained for the duration of its intended use.	Configure data retention policies in ad platforms to automatically delete data after the campaign ends (e.g., within 90 days).

NuSpark Media Group

GDPR CHECKLIST

INITIAL EMAIL

Checklist	Rationale	How
- Ensure recipients have provided express or implied consent before sending emails.	CASL requires express consent or valid implied consent (e.g., existing business relationship).	Collect consent through online forms with a checkbox for opting in or verify implied consent through previous interactions or transactions.
- Avoid using pre-checked consent boxes.	Pre-checked boxes do not meet CASL's standard of explicit and intentional consent.	Set checkboxes in forms to be unchecked by default using HTML form settings (<input type="checkbox" />).
- Clearly identify your company and include contact information in the email footer.	Transparency ensures recipients can easily recognize the sender and contact them if needed.	Add your company name, address, and a support email or phone number in the email footer.
- Provide a clear and simple unsubscribe mechanism in every email.	CASL requires recipients to have an easy way to opt out of communications.	Include a visible unsubscribe link in the email, which redirects users to a page confirming their opt-out or preference change.
- Ensure the subject line and email content are not misleading.	CASL prohibits deceptive practices, ensuring truthful communication is essential.	Review subject lines and email content for accuracy and relevancy to the recipient's interests or consent.
- Keep records of consent, including timestamps and the method of obtaining consent.	Provides evidence of compliance if requested by regulators.	Use a CRM or consent management tool to log the details of consent, including timestamps and the opt-in method.
- Avoid sending emails to individuals who have opted out or whose implied consent period has expired.	CASL specifies time limits for implied consent (e.g., 2 years for existing business relationships).	Regularly audit your email list to remove contacts who have opted out or whose implied consent period has expired.