

Durable medium: digital-by-default (MiFID retail disclosures)



Effective 12 Jan 2026

Checklist for delivery controls, evidence, and customer options

Delivery controls	Evidence	Customer options
<ul style="list-style-type: none"> Match customer identity to email address (reduce mis-delivery) 	<ul style="list-style-type: none"> Store the exact issued disclosure (or verifiable copy) 	<ul style="list-style-type: none"> Make paper available on request (clear + friction-light)
<ul style="list-style-type: none"> Protect sensitive disclosures (encryption + access controls) 	<ul style="list-style-type: none"> Capture who (customer ref + destination address) 	<ul style="list-style-type: none"> Record and honour preferences (and keep them updated)
<ul style="list-style-type: none"> Use step-up authentication where risk warrants it (e.g., multi-factor, IDV) 	<ul style="list-style-type: none"> Capture when (issue time + delivery attempts) 	<ul style="list-style-type: none"> Support alternative formats (accessibility/vulnerability needs)
<ul style="list-style-type: none"> Avoid “live” links to files - store a fixed, versioned copy of what you sent 	<ul style="list-style-type: none"> Capture how (channel + any authentication applied) 	<ul style="list-style-type: none"> Log channel switches (and why the method was appropriate)
<ul style="list-style-type: none"> Define failure handling (bounces, invalid addresses, repeated non-delivery) 	<ul style="list-style-type: none"> Record status + follow-up actions (delivered / bounced / failed + what happened next) 	<ul style="list-style-type: none"> Ensure service teams can manage options day-to-day (not “Compliance-only”)

Digital-by-default does not remove durable medium expectations - you still need client control, retention, and persistence for information you send.