Summary of the Recommended Protective Measures for EIOPA Information

Confidentiality Level	Information Exchange with EIOPA	Internal Distribution		External Distribution		Handling and Storage		Disposal	
		Paper documents	**Electronic format**	**Paper documents**	**Electronic format**	**Paper documents**	**Electronic format**	**Paper documents**	**Electronic format**
EIOPA REGULAR USE	No restrictions Email permitted	No restrictions if done in relation with a public function		Seek EIOPA's prior consent		No restrictions on storage or disposal			
EIOPA RESTRICTED USE	EIOPA Extranet and HUB whenever possible Email permitted	On a need to know basis Internal mail Hand delivery	Document management systems Links to documents whenever possible	Seek EIOPA's prior consent National post service or courier Hand delivery	Encryption whenever possible Collaboration platforms with access control and encryption preferred Email permitted	Locked cupboards Locked rooms Clean desk policy	Document management systems and repositories with access control and adequate security controls Encryption at rest on mobile devices and removable media	Shredding Locked confidential waste disposal container Physical destruction	Secure deletion
EIOPA CONFIDENTIAL USE	EIOPA Extranet EIOPA HUB Email (TLS) encryption	On a need to know basis Should be kept to a minimum Internal mail Hand delivery Sealed envelope	Document management systems Links to documents whenever possible	Seek EIOPA's prior consent Registered mail or courier services Hand delivery against signature Double envelope	Encryption mandatory Collaboration platforms with access control and encryption Encrypted email	Locked cupboards or safes Locked rooms Clean desk policy	Document management systems and repositories with access control and adequate security controls Encrypted at rest on mobile devices and removable media	Cross-cut shredding Locked confidential waste disposal container Physical destruction	Secure deletion