交通部　公告　　中華民國 113 年 12 月 23 日
交運字第 11312089171 號

主　　旨：預告訂定「鐵路運輸業個人資料檔案安全維護管理辦法」。

依　　據：行政程序法第一百五十四條第一項。

公告事項：

一、修正機關：交通部。

二、修正依據：個人資料保護法第二十七條第三項。

三、「鐵路運輸業個人資料檔案安全維護管理辦法」草案如附件。本案另載於本部全球資訊網（網址：https://www.motc.gov.tw），「政策、法規與研究－法規即時檢索－草案預告區」網頁及公共政策網路參與平臺「眾開講」（網址：https://join.gov.tw/policies/index）之「法令草案預告」。

四、對於本公告內容有任何意見或修正建議者，請於本公告刊登公報隔日起 60 日內陳述意見或洽詢：

（一）承辦單位：交通部鐵道局。

（二）地址：新北市板橋區縣民大道二段 7 號 9 樓。

（三）聯絡人：傅專員。

（四）電話：（02）8072-3333 分機 1505。

（五）傳真：（02）8969-1519。

（六）電子郵件：msl_fu@rb.gov.tw。

鐵路運輸業個人資料檔案安全維護管理辦法草案總說明

有鑑於鐵路運輸業者因業務需求，蒐集持有消費者之個人資料，為有效保護該些個人資料以防止個人資料被竊取、竄改、毀損、滅失或洩漏，對業者所保有之個人資料檔案，應採行適當之安全措施，爰依個人資料保護法第二十七條第三項規定，訂定鐵路運輸業個人資料檔案安全維護管理辦法（以下簡稱本辦法），共計二十三條，其要點如下：

一、本辦法之適用對象。（第二條）

二、業者應訂定安全維護計畫及公開個人資料保護管理政策，並指定專人或建立專責組織負責訂定、修正及執行。（第三條）

三、業者應界定個人資料之範圍，進行個人資料之風險評估及管理，規劃事故之預防、通報及應變機制。（第四條至第六條）

四、業者應實施個人資料蒐集、處理或利用之內部管理程序應辦理事項。（第七條至第十四條）

五、有關人員管理、資料安全管理、資通系統資訊安全措施、環境管理及業務終止後個人資料處理方法等事項。（第十五條至第十八條）

六、有關資料安全稽核機制、紀錄保存及整體持續改善等事項。（第十九條至第二十二條）

鐵路運輸業個人資料檔案安全維護管理辦法草案

條　文	說　明
第一條　本辦法依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定之。	本辦法之訂定依據。
第二條　本辦法適用對象為經營傳統鐵路經營業及高速鐵路經營業之鐵路運輸業(以下簡稱業者）。 業者應依其業務規模及特性，衡酌經營資源之合理分配，規劃、訂定、檢討與修正安全維護措施，並納入個人資料檔案安全維護計畫（以下簡稱安維計畫)，以落實個人資料檔案之安全維護與管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 安維計畫之內容應包括第三條至第二十二條規定之相關組織及程序，並應定期檢視及配合相關法令修正。 業者應於本辦法施行之日起六個月內，完成安維計畫之訂定，報請交通部備查，修正時亦同。	一、第一項明定本辦法之適用對象，目前屬非公務機關之鐵路運輸業為國營臺灣鐵路股份有限公司(傳統鐵路經營業）及台灣高速鐵路股份有限公司(高速鐵路經營業）。 二、依本法第二十七條第二項規定及本法施行細則第十二條規定，交通部得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法，於第二項明定業者應配置相當資源，俾規劃、訂定、檢討、修正與執行安維計畫之相關事項，落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 三、第三項明定安維計畫之具體內容。 四、為監督業者建立相關個人資料檔案安全維護管理機制，爰於第四項明定業者應於本辦法發布施行之日起六個月內完成安維計畫之訂定，並報請鐵路運輸業之中央目的事業主管機關交通部備查，修正時亦同。
第三條　業者就個人資料檔案安全維護管理應指定專人或建立專責組織，並配置相當資源。 前項專人或專責組織之任務如下： 一、訂定、修正與執行安維計畫及業務終止後個人資料處理方法等相關事項。 二、訂定個人資料保護管理政策，將其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保	參考本法施行細則第十二條第二項第一款及第七款規定，適當安全維護措施得包括配置管理之人員及相當資源、認知宣導及教育訓練，為使相關業者落實個人資料檔案安全之保護措施，明定業者應指定專人或建立專責組織；並明定專人或專責組織除負責安維計畫相關事項外，亦須對所屬人員進行教育訓練，使其明瞭個人資料保護法相關規定、所屬人員之責任範圍。

護事項，公告使其所屬人員均明確瞭解。 三、定期對所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令之規定、所屬人員之責任範圍及各種個人資料保護事項之方法或管理措施。	
第四條　業者應清查所保有之個人資料，界定其納入安維計畫之範圍並建立檔案，且定期確認有無變動。 前項清查發現下列情形者，業者應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料： 一、非屬特定目的必要範圍內之個人資料。 二、特定目的消失或期限屆滿而無本法第十一條第三項但書之情形。	一、參考本法施行細則第十二條第二項第二款規定，適當安全維護措施得包括界定個人資料之範圍，為使相關業者落實個人資料檔案安全之保護措施，於第一項明定業者應瞭解其所蒐集、處理及利用之個人資料，掌握其保有個人資料之內涵，如個人資料檔案名稱、個人資料類別等，以便有效規劃個人資料保護事項，及瞭解其所蒐集、處理及利用之個人資料是否合法，是否符合所適用個人資料保護之有關法令現況。 二、蒐集、處理或利用個人資料，均應於特定目的必要範圍內為之，若蒐集、處理、利用個人資料之特定目的已消失或期限已屆滿，而無本法第十一條第三項但書之情形者，依本法第十一條第三項規定，應予以刪除、停止處理或利用，爰訂定第二項規定。
第五條　業者應依據前條所界定之個人資料範圍及其相關業務流程，分析可能產生之風險，並依據風險分析結果，訂定適當管控措施。	參考本法施行細則第十二條第二項第三款規定，適當安全維護措施得包括個人資料之風險評估及風險管理，為使相關業者落實個人資料檔案安全之保護措施，明定業者應依據其相關業務流程，判斷蒐集、處理及利用個人資料之過程中，個人資料安全可能發生之風險及其風險性之高低，並進一步以適當方式保護之。
第六條　業者為因應所保有之個人資料被竊取、竄改、毀損、滅失、洩漏或其他侵害情形（以下簡稱事故），應採取	一、參考本法施行細則第十二條第二項第四款規定，適當安全維護措施得包括事故之預防、通報及應變機制，

下列事項： 一、適當之應變措施，以控制事故對當事人之損害。 二、查明事故之狀況並以適當方式通知當事人；其通知內容包含個人資料發生事故之事實、業者所採取之因應措施及所提供之諮詢服務專線。 三、研訂預防機制，避免類似事故再次發生。 業者應於發現前項事故後七十二小時內填具個人資料侵害事故通報及紀錄表（如附表）通報交通部鐵道局確認後轉報交通部；其屬重大矚目事故案件者，應於二十四小時內完成前述通報作業。未於時限內通報者，應附延遲理由。 重大矚目事故案件，其範圍如下： 一、行政院、立法院或監察院關注之個人資料事故。 二、經媒體顯著披露之個人資料事故（如經平面媒體全國性版面報導、電子媒體專題討論）。 交通部接獲第二項通報後，得依本法第二十二條至第二十六條規定，為適當之監督管理措施。	為降低或控制因個人資料被竊取、竄改、損毀、滅失、洩漏或其他侵害情形等事故造成資料當事人財產及非財產上之損害，為使相關業者落實個人資料檔案安全之保護措施，於第一項明定業者應訂定相關因應機制及必要作為。其中第二款之「以適當方式通知當事人」，依本法第十二條及本法施行細則第二十二條規定，指業者應即時以電子郵件、簡訊、電話或其他足以使當事人知悉或可得知悉之方式，通知當事人事故之發生與處理情形，及後續供當事人查詢之電話專線或其他適當管道。 二、為期業者可藉由對交通部之事故通報，充分掌握個人資料事故發生原因，並予以妥善處理，進而控制個人資料事故造成之損害並防止復發，參考行政院及所屬各機關落實個人資料保護聯繫作業要點第五點第一項第三款，於第二項規定業者遇個人資料事故時，應於時限內通報交通部鐵道局確認後轉報交通部。 三、依行政院及所屬各機關落實個人資料保護聯繫作業要點第二點第二項，於第三項規定重大矚目事故案件之定義。 四、交通部得視實際需求依本法第二十二條至第二十六條規定採取相關行政作為，爰訂定第四項規定。
第七條　業者就個人資料蒐集、處理及利用之內部管理程序，應依下列事項辦理： 一、檢視及確認所蒐集、處理及利用之個人資料是否包含本法第六條所定個人資料及其特定目的。 二、檢視蒐集、處理及利用本法第六	一、參考本法施行細則第十二條第二項第五款規定，適當安全維護措施得包括個人資料蒐集、處理及利用之內部管理程序，俾使業者落實個人資料相關管理程序。 二、又依本法第六條所定特種個人資料較為特殊或具敏感性，業者原則不

條所定個人資料，是否符合相關法令之要件。 三、雖非本法第六條所定個人資料，其有特別管理之需要者，得比照或訂定特別管理程序。	得蒐集、處理及利用，並應依個人資料之屬性分別建立管理程序，以應確保蒐集、處理及利用個人資料，符合相關法令之要求。
第八條　業者為遵守本法第八條及第九條關於告知義務之規定，應採取下列方式： 一、檢視蒐集、處理個人資料之特定目的，是否符合免告知當事人之事由。 二、依據資料蒐集之情況，採取適當之告知方式。	一、依本法第八條及第九條規定，業者原則應適時履行告知義務，除經檢視有符合例外無須告知之事由外，依據資料蒐集情形，應採取適當告知方式，以確實履行告知義務。 二、又依本法施行細則第十六條所稱適當方式通知當事人，係指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。
第九條　業者應檢視蒐集、處理個人資料是否符合本法第十九條規定，具有特定目的及法定要件。 業者應檢視利用個人資料是否符合本法第二十條第一項規定，符合特定目的內利用；於特定目的外利用個人資料時，應檢視是否具備法定特定目的外利用要件。	參考本法施行細則第十二條第二項第五款規定，安全維護措施得包括個人資料蒐集、處理及利用之內部管理程序，為使相關業者落實個人資料檔案安全之保護措施，明定業者應遵循本法有關蒐集、處理及利用個人資料之特定目的及法定要件，以利個人資料安全維護。
第十條　業者於首次利用個人資料行銷時，應提供當事人免費表示拒絕行銷之方式；當事人表示拒絕行銷後，應立即停止利用其個人資料行銷，並周知所屬人員。	為維護當事人資料之權益，以符合本法第二十條第二項及第三項規定，明定業者應提供當事人表示拒絕接受行銷之方式。
第十一條　交通部依本法第二十一條規定，對業者為限制國際傳輸個人資料之命令或處分時，業者應通知所屬人員遵循辦理。 業者將個人資料作國際傳輸者，應檢視是否受交通部限制，並告知當事人其個人資料所欲國際傳輸之區域，且對資料接收方為下列事項之監督： 一、預定處理或利用個人資料之範	一、第一項明定依本法第二十一條規定所為之命令或處分，業者應通知所屬人員知曉並遵照辦理。 二、第二項明定業者將個人資料作國際傳輸者，應檢視是否受中央目的事業主管機關交通部依本法第二十一條規定之命令或處分限制，並且告知個人資料所欲國際傳輸之區域，同時對資料接收方為相關之監督。

圍、類別、特定目的、期間、地區、對象及方式。 二、當事人行使本法第三條所定權利之相關事項。	
第十二條　業者委託他人蒐集、處理或利用個人資料之全部或一部時，應對受託者依本法施行細則第八條規定為適當之監督，並明確約定相關監督事項與方式。	依本法第四條規定：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關」；及本法施行細則第八條第一項規定：「委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督」，同條第二項並明定前項監督至少應包含事項。爰於本條重申前開規定意旨，提醒業者遵循。
第十三條　業者為提供資料當事人行使本法第三條所規定之權利，應採取下列方式為之： 一、確認是否為個人資料之本人，或經其委託授權。 二、提供當事人行使權利之方式，並遵守本法第十三條有關處理期限之規定。 三、告知是否酌收必要成本費用。 四、如認有本法第十條及第十一條得拒絕當事人行使權利之事由，應附理由通知當事人。	依本法第三條規定，當事人就其個人資料得行使查詢或請求閱覽、製給複製本、補充或更正、停止蒐集、處理或利用及刪除其個人資料等權利，且非公務機關除依本法第十條但書、第十一條第二項但書或第三項但書規定得拒絕當事人行使權利之情形外，應依當事人之請求辦理，並應於本法第十三條規定期間內准駁，爰明定業者應遵循辦理事項，以利資料當事人行使權利。
第十四條　業者為維護其所保有個人資料之正確性，應採取下列方式為之： 一、檢視個人資料於蒐集、處理或利用過程，是否正確。 二、當發現個人資料不正確時，適時更正或補充，並通知曾提供利用之對象。 三、個人資料正確性有爭議者，應依本法第十一條第二項規定處理。	業者所保有個人資料之正確性，攸關業者是否能有效利用個人資料以提供當事人相關服務，並避免當事人遭受因資料不正確而生之損害。因此，業者應採取相關方法，檢視個人資料之正確性，包含蒐集、處理或利用過程時，應檢視並登載資料確實，發現異狀時，採取更正之相關措施。
第十五條　業者應採取下列人員管理措施： 一、依據作業之需要，建立管理機制，設定所屬人員不同權限，並定期	參考本法施行細則第十二條第二項第六款規定，安全維護措施得包括資料安全管理及人員管理，為使相關業者落實個人資料檔案安全之保護措施，明定業者

確認權限內容之適當及必要性。 二、檢視各相關業務流程涉及蒐集、處理及利用個人資料之負責人員，俾落實負責人員管理。 三、與所屬人員約定保密義務。 四、所屬人員離職或完成指派工作後，應將其執行業務所持有之個人資料辦理交接，且不得私自持有複製物而繼續使用該個人資料。	應訂定從事個人資料業務之人員管理措施，諸如設定不同權限、簽訂保密條款、離職或完成受指派工作後應將個人資料交接，亦不得加以複製使用。
第十六條　業者應採取下列資料安全管理措施： 一、運用電腦或自動化機器相關設備蒐集、處理或利用個人資料時，應訂定使用可攜式設備或儲存媒體之規範。 二、針對所保有之個人資料內容，如有加密之需要，於蒐集、處理或利用時，應採取適當之加密機制。 三、作業過程有備份個人資料之需要時，應比照原件，依本法規定予以保護之。 四、個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物，嗣該媒介物於報廢或轉作其他用途時，應採適當防範措施，以免由該媒介物洩漏個人資料；其委託他人執行者，準用第十二條規定辦理。	參考本法施行細則第十二條第二項第六款規定，安全維護措施得包括資料安全管理及人員管理，為使相關業者落實個人資料檔案安全之保護措施，明定業者應對個人資料採取適當之資料安全管理措施，諸如加密、個人資料報廢或轉作其他用途時，應採取適當防範措施，避免洩漏個人資料。
第十七條　業者因執行業務以資通訊系統蒐集、處理或利用個人資料時，應採取下列資訊安全管理措施： 一、使用者身分確認及保護機制。 二、個人資料顯示之隱碼機制。 三、網際網路傳輸之安全加密機制。 四、個人資料檔案及資料庫之存取控制與保護監控措施。 五、防止外部網路入侵對策。	一、參考本法施行細則第十二條第二項第六款規定，安全維護措施得包括資料安全管理及人員管理，為使相關業者落實個人資料檔案安全之保護措施，於第一項明定業者蒐集、處理或利用個人資料檔案時，應依據個人資料風險評估之結果，於安維計畫訂定相關資料安全管理措施，防止個人資料被竊取、竄改、毀損、

六、非法或異常使用行為之監控與因應機制。 前項第五款及第六款所定措施，應定期演練及檢討改善。	滅失或洩漏。其中第二款之隱碼機制，業者評估使用情境以決定是否以及如何採取適當之隱碼措施。 二、第二項明定業者應定期演練前項第五款及第六款所定措施，以及時發現問題並檢討改善。
第十八條　業者針對保有個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦或自動化機器設備等媒介物之環境，應採取下列環境管理措施： 一、依據作業內容之不同，實施適宜之進出管制方式。 二、所屬人員妥善保管個人資料之儲存媒介物。 三、針對不同媒介物存在之環境，審酌建置適度之保護設備或技術。	參考本法施行細則第十二條第二項第八款規定，安全維護措施得包括設備安全管理，為使相關業者落實個人資料檔案安全之保護措施，明定業者蒐集、處理或利用個人資料檔案時，應依據個人資料風險評估結果，於安維計畫訂定相關設備安全管理措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏，包括業者用以保存個人資料之各類儲存媒介物，應具有一定保護程度之要求，例如一定程度之技術、設備、管制措施及安全環境等。
第十九條　業者應訂定個人資料安全稽核機制，定期或不定期查察是否落實執行所定之安維計畫或業務終止後個人資料處理方法等相關事項。	參考本法施行細則第十二條第二項第九款規定，為使相關業者落實個人資料檔案安全之保護措施，明定業者應於安維計畫，訂定個人資料安全稽核機制，並定期或不定期進行內部稽核。
第二十條　業者應採行適當措施，採取個人資料使用紀錄、留存自動化機器設備之軌跡資料或其他相關證據保存機制，以供必要時說明其所定計畫之執行情況；其相關紀錄之保存期限至少為五年。	參考本法施行細則第十二條第二項第十款規定，為使相關業者落實個人資料檔案安全之保護措施，明定業者應於安維計畫，訂定相關使用紀錄、軌跡資料及證據保存機制，妥善保存個人資料之蒐集、處理或利用紀錄、自動化機器設備之軌跡資料及落實個人資料檔案安維計畫之證據等；另其相關紀錄之保存期限，參照船舶運送業個人資料檔案安全維護計畫及處理辦法規定，明定業者應保存至少為五年。
第二十一條　業者宜參酌執行業務現況、社會輿情、技術發展、法令變化等因素，檢視所定之安維計畫是否合宜，必要時予以修正。	參考本法施行細則第十二條第二項第十一款規定，為使相關業者落實個人資料檔案安全之保護措施，明定業者宜參酌相關因素，檢視所定安維計畫是否合宜，俾利個人資料安全維護得持續滾動檢討

	改善。
第二十二條　業者於業務終止後，針對個人資料應依下列措施為之，並留存相關紀錄；其相關紀錄之保存期限至少為五年： 一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。 二、移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。 三、其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。	一、業者於業務終止後，自不得再繼續使用所保有之個人資料檔案，並應作妥善處置，爰明定終止業務者，應視其終止原因，將保有之個人資料予以銷毀、移轉或其他刪除處理或利用等方式處理；並明定業者銷毀、移轉或其他刪除處理或利用個人資料過程中，應保存處理方式、地點、時間、執行人員、接受移轉資料之對象及合法移轉依據等資料，以便日後得以提出舉證。 二、另其相關紀錄之保存期限，參照船舶運送業個人資料檔案安全維護計畫及處理辦法規定，明定業者應保存至少為五年。
第二十三條　本辦法自發布日施行。	本辦法施行日期。

第六條附表

規　定	說　明
個人資料侵害事故通報及紀錄表 非公務機關名稱 通報機關 通報時間：　年　月　日　時　分 通報人：　簽名(蓋章) 職稱： 電話： E-mail： 地址： 事件發生時間：　年　月　日　時　分 事件發生種類： □竊取 □洩漏 □竄改 □毀損 □滅失 □其他侵害情形 個資侵害之總筆數(大約):___筆 □一般個資_____筆 □特種個資_____筆 發生原因及事件摘要 損害狀況： 是否造成個資當事人財產損害： □是，財損金額_____元 □否 □其他損害情形，說明: 個人資料侵害可能結果 擬採取之因應措施 擬採通知當事人之時間及方式 個資侵害案件種類： □屬重大矚目之個資外洩案件 □屬一般個資外洩案件 若屬一般個資外洩案件，是否於發現個資侵害事故後72小時內通報： □是 □否，理由： 若屬重大矚目個資外洩案件，是否於發現個資侵害事故後24小時內通報： □是 □否，理由：	參考行政院及所屬各機關落實個人資料保護聯繫作業要點第七點第一項所定監督通報紀錄表，訂定本辦法之「個人資料侵害事故通報及紀錄表」。