EEA 個人データ保護規程

第Ⅰ部　　総則

第一条　　（目的および用途）

1.1　本規程(以下「本規程」という)は、GDPR が当社に適用される状況において、一般データ保護規則(以下「GDPR」という)の遵守を確保し、GDPR が適用される個人データ(第 2 条第 2 号に定義される)の国境を越えた移転に関する規則の遵守を確保することを目的とする。

1.2　本規程は、GDPR 以外の法に基づく当社の社内規程の内容を変更するものではない。

1.3　本規程と GDPR 以外の法に基づく当社の社内規程との間に矛盾がある場合は、より重い個人データの保護義務を課す規程が優先されるものとする。

1.4　本規程のうち、第Ⅱ部は GDPR が適用される個人データの処理にのみ適用される。

第二条　　（定義）

本規程において使用する用語の定義は、次のとおりとする:

(1)　「EEA 加盟国」とは、欧州経済領域内の国をいう。

(2)　「個人データ」とは、識別された自然人または識別可能な自然人(「データ主体」)に関する情報であって、氏名、識別番号、位置情報、オンライン識別子(IP アドレス、Cookie を含む)、または自然人の身体的、生理的、遺伝的、精神的、経済的、文化的もしくは社会的な同一性を示す 1 以上の要素を参照することにより、直接または間接に識別することができるものをいう。

(3)　「センシティブデータ」とは、人種的もしくは民族的出身、政治的意見、宗教的もしくは思想的信条、労働組合への加盟を明らかにする個人データ、遺伝情報、自然人を特定するための生体情報、健康に関するデータまたは自然人の性生活もしくは性的指向に関するデータを明らかにする個人データをいう。

(4)　「処理」とは、収集、記録、組織化、構造化、保管、修正または変更、検索、参照、使用、送信、配布による開示またはその他提供、整列または結合、制限、消去または破棄など、自動化された手段であるかどうかにかかわらず、個人データまたは個人データの集合に対して行われるあらゆる操作または一連の業務遂行を意味する。

第Ⅱ部　　GDPR が適用される個人データの処理について

第一章　　個人データの取扱いについて

第三条　　（個人データの取扱いに関する一般原則）

3.1　個人データは、以下の原則に従って処理されるものとする:

(1) データ主体との関係において、適法、公正かつ透明性のある方法で処理されること;

(2) 特定された、明確であり、かつ正当な目的のために収集されること、かつ、それらの目的と相容れない方法でさらに処理されることがないこと;

(3) 適切で、関連性があり、処理される目的との関係において必要な範囲に限定されていること;

(4) 正確かつ必要に応じて最新の状態に保たれていること;

(5) 個人データの処理目的に必要な期間に限り、データ主体を識別できる形で保持されること;

(6) 適切な技術的または組織的措置を用いて、個人データの適切なセキュリティを確保する方法で処理されること。

3.2 当社は、個人データ処理を、前 3.1 項に準拠して、実証可能な状態で維持する。

第四条 （個人データの処理）

個人データは、以下のいずれかに該当する場合を除き、処理されないものとする。:

(1) データ主体が、特定の目的のために個人データを処理することに同意している場合;

(2) データ主体が当事者となっている契約を履行するため、または契約を締結する前にデータ主体の要求に応じて措置を講じるために個人データの処理が必要となる場合;

(3) EU または EEA 加盟国の法令に定められた法的義務を順守するために処理が必要となる場合;

(4) データ主体または他の自然人の生命に関する利益を保護するために処理が必要となる場合;

(5) 当社または第三者が追求する正当な利益のために処理が必要である場合(ただし、個人データの保護を必要とするデータ主体の利益または基本的な権利および自由が、当該利益よりも優先される場合を除く。);

(6) その他、EEA 加盟国の法令に基づいて処理が許容される場合。特に雇用に関する目的で、採用の決定または採用後の雇用契約の履行、もしくは終了のために必要な場合;

(7) 収集された個人データにつき、収集した目的とは別の目的でさらなる処理を行う場合（ただし、当該追加的処理の前にデータ主体へ当該目的に関する情報提供を行う必要がある。）。

第五条　　（同意の条件）

個人データの処理が同意を法的根拠とする場合、その同意は、データ主体が当該処理について明確かつ具体的な説明を受けた上で、明確な積極的行為により自由に与えたものでなければならない。同意の撤回は、同意を与えるのと同じように容易でなければならない。当社はこれらについて証明できるようにしなければならない。

第六条　　（センシティブデータの処理）

6.1　第 4 条の規定にかかわらず、センシティブデータは、以下の場合を除き、処理されないものとする:

(1)　データ主体が、特定の目的のためにセンシティブデータが処理されることに対して明示的に同意した場合;

(2)　EU または EEA 加盟国の法令、またはデータ主体の基本的権利および利益に関連する適切な保護措置を規定する EEA 加盟国の法令に基づく労働協約により認められる範囲内で、雇用および社会保障ならびに社会的保護に関する法の分野において、当社もしくはデータ主体の義務を履行し、またはそれらの者の特定の権利を行使する目的のために処理が必要である場合;

(3)　データ主体が物理的または法的に同意を与えることができない場合で、データ主体または他の自然人の生命に関する利益を保護するために処理が必要である場合;

(4)　データ主体が明確に公表している個人データに関する処理の場合;

(5)　訴えの提起または法的主張に関する攻撃防御のために処理が必要である場合;

(6)　EU または EEA 加盟国の法令に基づき、または医療専門家との契約に基づいて、かつ、GDPR に定める条件および保護措置に従うことを条件として、従業者の業務遂行能力の評価、医療上の診断、医療もしくは社会的ケアまたは治療の提供、医療制度または社会福祉制度の管理もしくはそれらサービスの管理のために、処理が必要である場合;

(7)　その他、EEA 加盟国の法令に基づき処理が許可されている場合。

6.2　前 6.1 項(6)に定める「GDPR に定める条件」とは、センシティブデータが EU 法もしくは EEA 加盟国の国内法または加盟国の職務権限を有する機関により定められた規程に基づく職務上の秘密保持義務に服する専門家により、もしくは専門家の責任の下で処理されること、または、EU 法もしくは EEA 加盟国の国内法または加盟国の職務権限を有する機関により定められた規程に基づく秘密保持義務に従うその他の自然人によって取り扱われることを意味するものである。

第七条　　（データ主体からの個人データの収集）

7.1　データ主体から個人データを収集する場合には、原則として、当該収集に際して、下記各号の情報をデータ主体に提供する。

(1) 当社（および EU 代理人が選任されている場合は当該代理人）の名称および連絡先の詳細（並びにデータ保護オフィサーが選任されている場合はその連絡先の詳細）;

(2) 個人データの処理の目的および法的根拠;

(3) 個人データの処理が第 4 条第 6 号に基づく場合、当社または第三者が求める正当な利益;

(4) 個人データが第三者に提供される場合には、個人データの提供先または提供先の種類;

(5) 個人データを EEA 域外の第三国に所在する第三者に移転しようとする場合には、その旨および譲受人について欧州委員会による十分性認定の有無、第 11 条第 1 項第 2 号もしくは第 11 条第4項第 7 号に基づく移転の場合は、適切または適切な保護措置および当該保護措置の内容を記載した文書（第 11 条第 1 項第 2 号に基づく移転の場合は、標準契約約款）の写しを入手する方法;

(6) 個人データを保存する期間(それが難しい場合は、その期間を決定するために使用される基準);

(7) 個人データへのアクセス、個人データの訂正、消去、処理の制限、処理への異議を申し立てる権利、データポータビリティの権利が存在すること;

(8) 個人データの処理が第 4 条第 1 号または第 6 条第 1 項第 1 号(データ主体の同意)に基づくものであるときは、その撤回前の同意に基づく適法な処理に影響を及ぼすことなく、いつでも同意を撤回することができる権利が存在すること;

(9) 監督機関に苦情を申し立てる権利;

(10) 個人データの提供が法令上または契約上の要求事項であるか否か、または契約を締結するために必要な要件であるか否か、ならびにデータ主体が個人データを提供する義務を負うか否か、および当該データを提供しない場合に生じる可能性のある結果;

(11) プロファイリングを含む自動化された意思決定の存在、およびそれが存在する場合には、その決定に含まれている論理および当該処理のデータ主体への重要性、ならびにデータ主体に生じると想定される結果に関する意味のある情報。

7.2 収集された個人データにつき、収集した目的とは別の目的でさらなる処理を行う場合、当社は、当該追加処理が実施される前に、データ主体に対して、かかる他の目的に関する情報および前項第 6 号から第 11 号に定める情報を提供する。

7.3 前各項は、データ主体が既に前各項に定める情報を保有している場合には、適用しない。

第八条　　（データ主体以外の者からの個人データの収集）

8.1　データ主体以外の者から個人データを収集する場合には、収集時に、データ主体に対し、原則として、以下の各号に掲げる情報を提供する:

(1)　前条第 1 項第 1 号から第 9 号までおよび第 11 号に掲げる事項;

(2)　収集する個人データの種類

(3)　個人データの出所および該当する場合には、出所が公にアクセス可能である旨

8.2　前項に定める情報をデータ主体に提供する期間は、個人データを取得してから合理的な期間内とし、原則として 1 ヶ月以内とする。ただし、次の各号のいずれかに該当するときは、当該各号に定める時までとする。

(1)　個人データがデータ主体との連絡のために使用される場合は、遅くとも当該データ主体への最初の連絡の時点

(2)　第三者への個人データの提供を予定している場合にあっては、遅くとも、当該個人データが最初に提供された時点。

8.3　個人データを、取得した目的とは異なる目的でさらに処理する場合は、データ主体に対し、当該追加処理に先立って、他の処理目的に関する情報および第 1 項第 3 号、前条第 1 項第 6 号から第 9 号まで、および第 11 号に定める情報を提供するものとする。

8.4　前各項の規程は、次の各号のいずれかに該当する場合は適用されない:

(1)　データ主体が既にその情報を持っている場合;

(2)　当該情報の提供が不可能な場合、または提供のために不相応な努力を伴う場合;

(3)　情報の取得または開示の義務が、EU 法または EEA 加盟国の国内法によって明示的に定められており、データ主体の正当な利益を保護するための適切な手段を提供している場合;

(4)　EU 法または EEA 加盟国の国内法により規制されている職業上の秘密保持義務(法的な秘密保持義務を含む)に基づき、個人データの秘密を保持しなければならない場合。

第九条　　（共同管理者）

9.1　当社と共同して個人データ処理の目的および手段を決定する管理者を共同管理者という。当社および当社と共同して個人データ処理の目的および手段を決定する管理者が服すべきそれぞれの責任が EU 法 または加盟国の国内法によって定められていない場合、当社および当社と共同して個人データ処理の目的および手段を決定する管理者は、とりわけ第二章に定めるデータ主体の権利の行使に関する義務、第 7 条第1項および第8条第1項に規定する情報を提供する義務、並びにその他の義務を遵守するためのそれぞれの責任に

ついて、管理者間での合意により、透明性のある態様で定めなければならない。その合意においては、データ主体のための連絡先を指定できる。

9.2 第 1 項に規定する合意は、当社と共同して個人データ処理の目的および手段を決定する管理者およびデータ主体とのそれぞれの間における役割および関係を適正に反映するものとする。その合意の要点は、データ主体に利用可能なものでなければならない。

9.3 第 1 項に規定する合意に定める条件にかかわらず、データ主体は、当社と共同して個人データ処理の目的および手段を決定する管理者に対して、第 15 条第 1 項に基づく自己の権利を行使できる。

第十条 （個人データの処理の委託）

10.1 個人データの処理を第三者(当該処理を委託された相手方を「委託先」という。)に委託する場合、当社は、GDPR の要件を満たし、技術的および組織的措置を実施するための十分な保証を提供する委託先のみを用いることとし、かつ、委託先によるデータ主体の権利の保護を確実にしなければならない。

10.2 個人データ処理を外部の第三者に委託する場合は、委託先との間で、処理の対象および期間、処理の性質および目的、個人データの種類および区分、当社の義務および権利、ならびに委託先が次に掲げる事項を実施することを定めた契約を締結しなければならない。

(1) 委託先は、個人データの第三国への移転に関するものを含め、当社からの文書による指示に基づいてのみ個人データを処理すること。ただし、EU の法律または委託先が属する EEA 加盟国の法律により別段の措置を講じることが義務付けられている場合はこの限りではない。委託先は、個人データの処理が法律により要求される場合、当該法が公共の利益上の重要な法的根拠に基づいて情報提供を禁止する場合を除き、処理前に当該法律上の要件を当社に通知すること。;

(2) 委託先は、個人データを処理する権限を与えられた者が、自ら守秘義務を負うか、または適切な守秘義務の下にある状態を確保すること;

(3) 委託先は、第 14 条の規定に基づいて要求されるリスクに応じた、適切な技術的および組織的措置を実施すること;

(4) 委託先は、再委託する旨を当社へ事前に報告しなければならない。再委託に関する当社の事前承認を得たうえで、再委託先との間で契約を締結し、再委託先に対し、本項と同等のデータ保護に関する義務を課すこと。再委託先が当該義務を履行しない場合、委託先は、当社に対して全責任を負うこと;

(5) 委託先は、処理の性質を考慮し、当社が第 15 条に定めるデータ主体の権利の行使の要請に応じる義務を果たすために、可能な限り、適切な技術的および組織的措置により当社を支援すること;

(6) 委託先は、処理の性質および処理者が利用できる情報を考慮に入れて、当社が GDPR 第 32 条から第 36 条に基づく義務の順守を確保するために当社を支援すること;

(7) 委託先は、EU の法律または EEA 加盟国の法律によって個人データの保管が必要とされない限り、委託先における個人データの処理が完了した後、当社の選択に従い、すべての個人データを削除または当社に返却し既存のコピーを削除すること;

(8) 委託先は、本項に定める義務の遵守を実証するために必要なすべての情報を当社に提供し、当社または当社が委任する別の監査人が実施する監査を許可し、これに貢献すること。

第十一条 （個人データの国境を越えた移転）

11.1 EEA 域外の第三国にある第三者への個人データの移転は、以下のいずれかの場合にのみ行うことができる:

(1) 移転先となる EEA 域外の第三国に適用される、欧州委員会による十分性認定がある場合、または

(2) 欧州委員会により採択された標準契約条項(「SCC」)が、移転が行われる当事者が締結する契約に含まれており、当社が当該移転に伴うリスクを評価し、EEA におけるものと本質的に同等のレベルのデータ保護水準を確保するために必要な措置を講じている場合

11.2 前項の移転が十分性認定に基づくものである場合には、十分性認定に基づき移転される個人データの処理については、個人データの保護に関する法律の規定および当該処理に適用される十分性認定の補完的ルールに従う。

11.3 第 1 項に定める移転が SCC に依拠している場合、SCC に基づき移転された個人データの処理に関して、当社は、処理に適用される個人データの保護に関する法律の規定に従いつつ、SCC に基づく義務を履行する。

11.4 第1項各号のいずれにも該当しない場合であっても、次の各号のいずれかに該当する場合には、EEA 域外の第三国の第三者に個人データを移転することができる:

(1) データ主体が、十分性認定および SCC が存在しないことに伴ってデータ主体に生じうるリスクについて知らされた後、当該移転に明示的に同意した場合;

(2) データ主体と当社との間の契約の履行のために、またはデータ主体の要求に応じて契約を締結する前の手続きを取るために、移転が必要である場合;

(3) 当社と第三者との間でデータ主体の利益のために行う契約の締結または履行のために移転が必要である場合;

(4) 重要な公益上の理由により移転が必要である場合;

(5) 訴えの提起または法的主張に関する攻撃防御のために移転が必要である場合;

(6) データ主体が物理的または法的に同意を与えることができない場合で、データ主体またはその他の者の生命に関する利益を保護するために移転が必要である場合;

(7) 前項に基づいて移転を行うことができず、かつ、本項第1号から第6号による例外がいずれも適用されない場合、当社が追求する正当な利益(個人データの保護を求めるデータ主体の利益、権利および自由が優先する場合を除く)に基づいて、反復的ではなく、限定された数のデータ主体のみに移転する場合に限り、データ移転を取り巻くすべての状況を評価し、その評価に基づいて個人データの保護に関する適切な保護措置を提供している場合。

11.5 当社は、前項第 7 号に基づいて EEA 域外の第三者に個人データを移転する場合は、当該移転につき監督機関に通知するとともに、移転の対象となるデータ主体に対し、本件データ移転の事実および当社が追求する正当な利益について通知する。

第十二条 (処理活動の記録)

12.1 個人データの処理に関し、次の各号に掲げる事項について記録を作成し、これを保存する:

(1) 当社(ならびに共同管理者およびデータ保護オフィサーが選任されている場合はその者)の氏名および連絡先詳細;

(2) 処理の目的;

(3) データ主体のカテゴリーおよび当該個人データのカテゴリーの説明;

(4) 個人データの開示を受け、または受けようとする受領者の区分;

(5) 第三国への個人データの移転(第三国の特定を含む。)および第 11 条第 4 項第 7 号に掲げる移転の場合にあっては、適当な保障措置に関する書類;

(6) 個人データの区分ごとに想定される、個人データの消去期限;

(7) 第 14 条第 1 項に規定する技術的および組織的措置の概要説明。

12.2 前項の記録は、書面をもって作成し、これを保存する。

12.3 我々は、12.1 項に記載された記録を、要請があれば監督機関に提供する。

第十三条 (個人データの保存期間)

13.1 当社は、目的に照らして必要な範囲内で個人データを保管する。

13.2 当社は、個人データが収集時の目的に照らして必要であるかを定期的に確認し、不要と判断したデータを適切な方法で削除する。ただし、保管が法的に義務づけられている場合、法的請求または法的請求に対する防御のために保管の必要がある場合は、この限りでない。

13.3 前項の検証を実施した場合には、その概要を作成し、保管する。

第十四条　　（技術的および組織的措置）

14.1　当社は、技術水準、実施に要する費用並びに個人データの処理の性質、範囲、状況および目的、並びに自然人の権利および自由に対する様々な蓋然性と深刻度のリスクを考慮に入れたうえで、リスクに見合ったセキュリティレベルを確保するために、適切な技術的および組織的措置をしかるべく実施する。実施に際しては、以下の措置の可否を検討する。

(1)　個人データの仮名化・暗号化;

(2)　処理システムおよびサービスの継続的な機密性、完全性、可用性および耐障害性を確保する能力;

(3)　物理的または技術的なインシデントが発生した場合に、個人データの利用可能性およびアクセスを適時に回復する能力

(4)　処理の安全性を確保するための技術的および組織的措置の有効性を定期的にテストし、評価し、評価するためのプロセス。

14.2　当社は、GDPR の義務を履行し、データ主体の権利および自由を保護するために、処理の手段の決定時点および処理過程において、効果的な方法で、必要な保護措置を処理に統合するため、適切な技術的および組織的措置を実施する。当社は、組織的および技術的措置の定期的な見直しを行い、必要に応じて新たな措置を実施する。

14.3　当社は、次に掲げる事項を考慮し、個人データが本人の関与なしに不特定多数の自然人によってアクセスされないようにすることを含め、処理の特定の目的ごとに必要な個人データのみが処理されることをデフォルトで確保するための適切な技術的および組織的措置を実施する。

(1)　収集した個人データの量;

(2)　個人データの処理の範囲;

(3)　個人データの保管期間;

(4)　個人データへのアクセス可能性。

14.4　データ主体の権利および自由を侵害する高いリスクをもたらす可能性がある個人データの処理を新たに行う場合、上記第 1 項に定める技術的および組織的措置の一環として、GDPR に基づくデータ保護影響評価を事前に実施するものとする。当社は、データ保護影響評価を行う場合、データ保護オフィサーに対して助言を求めなければならない。

第二章　　データ主体の権利行使に対する措置

第十五条　　（データ主体による権利の行使）

15.1　当社は、当社が個人データを処理するデータ主体が GDPR で認められる範囲で行う、以下に列挙される要求を受けいれるものとする:

(1) 個人データの処理の有無の確認、個人データの閲覧の請求および個人データの複製の提供;

(2) 不正確な個人データの是正要求;

(3) 個人データの消去請求;

(4) 個人データの処理制限の請求;

(5) 当該個人データについて、構造化され、一般的に使用され、かつ、機械で読取可能な様式で個人データを受け取る権利の請求または他の事業者への移転の請求;

(6) 個人データの処理に対する異議申立

15.2 データ主体が前項の権利を行使する場合、当社は、いかなる場合もデータ主体からの要求を受け取ってから不当な遅滞なく(原則として 1 ヶ月以内)これに対処する。データ主体の本人確認ができない場合に限り、当社はデータ主体からの要求を拒否することができる。当社は、必要があるときは、その要求の複雑性および数量を考慮に入れた上で、さらに 2 か月延長することができる。当社は、データ主体に対し、その要求を受けた時から 1 か月以内に、その遅延の理由と共に、その期間延長を通知する。

第三章 個人データ侵害への対応

第十六条 (個人データ侵害)

16.1 当社は、個人データ侵害(送信、保管その他の処理をした個人データの偶発的または不法な破棄、紛失、改ざん、不正開示またはアクセスにつながるセキュリティ違反を総称していう。以下同じ)のおそれがある場合、本条に従って適切に対処する。

16.2 当該個人データ侵害により、データ主体の権利および自由が侵害されるおそれが高いと判断された場合には、当社は、原則としてその事実を知った後 72 時間以内に、当該個人データ侵害を所管の監督機関に通知する。監督機関への通知を 72 時間以内に実施できない場合は、遅滞にかかる理由を付して通知する。

16.3 個人データ侵害により、データ主体の権利と自由が著しく損なわれるおそれがあると当社が判断した場合には、当社は、不当に遅滞することなく、当該データ主体に当該個人データ侵害を通知する。

16.4 当社は、個人データ侵害があった場合には、その記録を作成し、適切に保管する。

第 III 部 雑則

第十七条 (懲戒)

この規程に違反した場合は、懲戒を含む人事上必要な措置を講じます。

附則

1. Daido Steel Group Europe GmbH は、本規程の内容、制定、改廃について責任を負うものとする。

2. 本規程は、01.12.2022 にて実施する。

3. 制定・改廃年月日
確立: 01.12.2022